

SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report
2010–2011

CA1
SIR
- A56

Checks and Balances

Viewing Security Intelligence
Through the Lens of Accountability





Security Intelligence Review Committee
P.O. Box 2430, Station D
Ottawa, ON K1P 5W5
613-990-8441

Visit us online at www.sirc-csars.gc.ca

© Public Works and Government Services Canada 2011
Catalogue No. PS 105-2011
ISSN 1921-0566



September 30, 2011

The Honourable Vic Toews
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Minister:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2010–2011, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

A stylized, handwritten signature in dark ink, appearing to be 'A. Porter'.

Arthur T. Porter, P.C., M.D.
Chair

A handwritten signature in dark ink, appearing to be 'Frances Lankin'.

Frances Lankin, P.C.

A handwritten signature in dark ink, appearing to be 'Philippe Couillard'.

Philippe Couillard, P.C., M.D.

A handwritten signature in dark ink, appearing to be 'Carol Skelton'.

Carol Skelton, P.C.

A handwritten signature in dark ink, appearing to be 'Denis Losier'.

Denis Losier, P.C.

About SIRC

The Security Intelligence Review Committee (SIRC, or the Committee) is an independent review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS, or the Service). It conducts reviews of CSIS activities and investigates complaints from the public about the Service. In doing so, SIRC provides assurance to Parliament and to all citizens of Canada that the Service investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians. For more information on SIRC, consult www.sirc-csars.gc.ca.

About CSIS

The Canadian Security Intelligence Service (CSIS) is responsible for investigating threats to Canada, analyzing information and producing intelligence.

To protect Canada and its citizens, CSIS advises the Government of Canada on issues and activities that are, or may pose, a threat to national security. It also provides security assessments to all federal departments and agencies, with the exception of the Royal Canadian Mounted Police.

A legal framework for both SIRC and CSIS

By virtue of the *CSIS Act*, Canada became one of the first democratic governments anywhere in the world to establish a legal framework for its security service. With this *Act*, Canada clearly defined in law the mandate and limits of state power to conduct security intelligence, and created accountability mechanisms to keep those considerable state powers in check—a model that, by and large, has stood the test of time.

Contents

MESSAGE FROM THE COMMITTEE MEMBERS.....	2
ABOUT THIS REPORT	4
SECTION 1: THE YEAR IN REVIEW.....	5
SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS	9
A. Reviews	9
CSIS's Use of the Internet.....	12
CSIS's Private Sector Relationships.....	13
CSIS's Intelligence-to-Evidence Process	15
CSIS's Investigation of Cyber Threats	17
CSIS's Relationship with a "Five Eyes" Partner.....	19
The Role of CSIS in the Interviews of Afghan Detainees.....	21
How CSIS Evaluates the Reliability of Human Sources	23
B. Complaints	25
Alleged Improper Conduct by CSIS	27
Alleged Delay in Providing a Security Assessment	28
Alleged Unjust, Unfounded and Unethical Assessment of an Applicant for Permanent Residency.....	29
SECTION 3: SIRC AT A GLANCE.....	30
Committee Membership	30
Staffing and Organization	30
Committee Activities	31
List of SIRC Recommendations	32

Message from the Committee Members

Building and maintaining trust in public institutions are tenets of a free, democratic society. This task is especially challenging when an institution cannot be subject to rigorous public scrutiny because much of its work must be carried out under the veil of secrecy. Such is the case with the Canadian Security Intelligence Service (CSIS), which has a responsibility to collect intelligence relating to threats to Canada's national security.

For over 25 years, the Security Intelligence Review Committee (SIRC) has worked to ensure that this powerful organization is accountable to Parliament and to the citizens of Canada. The same legislation that established the legal authority for CSIS's activities also created an elaborate system of checks and balances on its powers. SIRC's role, therefore, is to help ensure that the Service respects the fundamental rights and freedoms of Canadians while it investigates threats to national security.

Specifically, SIRC strives to ensure that CSIS carries out its duties in a lawful, effective and appropriate manner. It does so through continuous review of CSIS's activities and through the investigation of complaints against the Service, and by making findings and recommendations to the Minister of Public Safety and the Director of the Service. Our work is summarized, to the fullest extent permitted by law, in this annual report.

Although the Service's mandate has remained unchanged since its creation, CSIS's work has taken on a complexity not foreseen 25 years ago—unavoidably so, in a world where international threats emerge and proliferate at sometimes dizzying speed.

While SIRC has adjusted the way it deploys its resources to meet these altered circumstances, we have not strayed from the basic tasks set for us in 1984 by Parliament. As we see it, our job is to make independent, meticulous and fair-minded assessments of the facts as we find them, and to provide cogent advice and recommendations to government based on those assessments.

Amidst the shifting sands of public opinion, and the rapid pace of international events and change, SIRC's role and composition take on special importance. As Members, we bring considerable and diverse expertise to our work, having served in a variety of public sector fields—politics, medicine, public administration and NGOs, to name a few. That expertise gives us a collective awareness of—and sensitivity to—matters of public importance, while our arm's-length status means that we can act in a scrupulously non-partisan fashion. Canadians expect our work to transcend events and politics, and we will remain vigilant to ensure that it does.

This year's report aims once again to engage parliamentarians and indeed, all Canadians, on a number of important issues relevant to security intelligence. These are highlighted in *The Year in Review* and *Summaries of SIRC Reviews and Complaints* (Sections 1 and 2 of this annual report, respectively). We hope to advance the goal set out in last year's report: to generate public discussion on the future role and challenges of security intelligence, as well as the review function in support of that role.

In today's heightened threat environment, it is important that Canada's security intelligence service has the authority and capacity to investigate new threats. Equally important, those activities need to be carried out within a framework that provides proper accountability. Collective security must not come at the expense of individual rights and freedoms, and SIRC will maintain that clear principle at the forefront of its work.



Members of SIRC (from left to right):

The Honourable Denis Losier, The Honourable Frances Lankin, The Honourable Dr. Arthur T. Porter (Chair), The Honourable Dr. Philippe Couillard and The Honourable Carol Skelton.

About This Report

SIRC derives its mandate and functions from the same law that sets out the Service’s legal framework: the *Canadian Security Intelligence Service Act*. In accordance with this legislation, SIRC annually prepares a public report of its activities, which is tabled before Parliament by the Minister of Public Safety.

This annual report summarizes SIRC’s key analyses, findings and recommendations arising from its reviews and complaints investigations. It has three sections:

Section 1

The Year in Review

An analysis of prominent developments in security intelligence and how these relate to select findings and recommendations by SIRC from the previous year.

Section 2

Summaries of SIRC Reviews and Complaints

A synopsis of the reviews completed by SIRC, as well as the complaint reports issued during the fiscal year covered by this annual report.

Section 3

SIRC at a Glance

Highlights the public engagement, liaison and administrative activities of SIRC. This includes details of its annual budget and expenditures.

SECTION 1:

The Year in Review

This year, SIRC expanded its public engagement activities in pursuit of a goal we set out in our 2009–2010 Annual Report: to stimulate public discussion on the future role of security intelligence and, as a corollary, the review function in support of that role. Again and again, these discussions touched on one theme: that, in the aftermath of 9/11, Canada has seen greatly enhanced operational cooperation among the almost two dozen federal departments involved in national security.

Yet Canada's system of checks and balances, designed decades ago to ensure the accountability of individual agencies, has not kept pace with these changes. The existing review mechanisms—including SIRC—are neither configured nor equipped to examine fully Canada's increasingly integrated national security activities. At the same time, many departments and agencies currently involved in national security are not subject to any form of independent review.

Review of Canada's national security activities

Three commissions of inquiry—O'Connor, Iacobucci and Major—have reported in the past five years on matters relating to Canada's national security activities, and all have come to the same conclusion.

The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (also known as the O'Connor Commission), in particular, undertook an in-depth examination of Canada's national security accountability framework. Mr. Justice O'Connor proposed a greatly expanded role for SIRC, given its longstanding expertise in the review of national security activities. SIRC's new role would encompass ongoing, independent review of the national security activities of four departments in addition to CSIS, specifically the Department of Foreign Affairs and International Trade Canada (DFAIT), the Financial Transactions and Reports Analysis Centre (FINTRAC), Citizenship and Immigration Canada (CIC) and Transport Canada.

The key question in our minds is this: do these activities warrant permanent, independent and ongoing review? The national security activities of other federal entities certainly have the potential to have an impact on individuals. For example, Canada Border Services Agency (CBSA) can refuse a person entry into Canada, and CIC has the power to remove someone from Canada. Yet these powers do not compare to CSIS's capacity to collect intelligence in secrecy—activities that may have a direct impact on individuals' civil rights and liberties, but without their knowledge. CSIS's robust review mechanisms were designed as a

counterweight to the Service's ability to act covertly and in ways that can profoundly affect individual lives. Accordingly, we question whether the same level of permanent and independent review is required for departments and agencies whose mandates do not provide similar powers.

Looking ahead—retooling SIRC

The *CSIS Act*, which provides SIRC with the power and ability to review thoroughly every aspect of CSIS's activities and operations, is not broken. Still, the nature and extent of change within the security intelligence environment causes us to reflect on Canada's national security accountability structure and SIRC's role within it.

Justice O'Connor observed correctly that the national security activities of many federal entities have become largely intertwined in the aftermath of 9/11. SIRC's recent reviews have underscored this finding. CSIS now liaises and works closely with numerous federal partners on a daily basis, a trend that will likely intensify as the Service pursues a more active and intricate domestic and foreign agenda. CSIS's activities are examined exhaustively and reported on by SIRC through its reviews and investigation of complaints. The challenge is to provide Canadians with the same level of reassurance about all of the government's national security operations, writ large.

We believe that independent review of Canada's national security activities could be enhanced by retooling SIRC—achievable without major legislative amendments, expense or restructuring. This would allow for a proportionate yet effective system of broad, independent review for national security.

At present, in the context of reviews, SIRC cannot examine and assess national security matters that go beyond CSIS—even though they may be influenced by the Service's actions or advice. A slight adjustment to SIRC's mandate could address this gap, allowing for more comprehensive reviews of CSIS's information-sharing and interactions with domestic partners. Further, it would enable SIRC to examine the actions of other federal entities when they connect with, or relate to, CSIS. Additionally, a minor amendment to the *CSIS Act* could permit SIRC—at the request of the Minister of Public Safety and with the concurrence of the appropriate Minister—to undertake a national security review of an agency or agencies other than CSIS. These modest changes would be cost-effective, and could help to alleviate public concerns regarding Canada's existing system of national security accountability.

This year's review of CSIS's role in interviewing Afghan detainees is a case in point. SIRC's ability to review the actions of other involved departments would have resulted in a more comprehensive examination and, by the same stroke, helped to build a broader public account of Canada's national security activities abroad. Whether or not structural change occurs, SIRC will continue to ensure that its reviews provide the fullest assessment possible of CSIS's activities.

SIRC'S observations

SIRC has responded to the changing national security environment by looking at CSIS's operational activities in novel ways, and delving into new lines of inquiry. SIRC also is committed to making its work and findings public to the fullest extent possible as a way of contributing to the public discussion on national security.

In this spirit, this year featured several “baseline” reviews on new topics, including one that focused on the evolving nature of CSIS’s interactions with the private sector. Although SIRC regularly examines CSIS’s relationships with domestic and foreign counterparts and other public sector partners, we chose for the first time to take an in-depth look at CSIS’s cooperation with the private sector. The review concluded that, despite the impetus towards greater cooperation with the private sector, especially with the owners and operators of some of the nation’s critical infrastructure, there are significant legal and practical limitations on the Service’s ability to work closely with the private sector.

Of note, the review revealed an emerging gap between CSIS’s legal framework, created three decades ago during the height of the Cold War, and the post-9/11 operational reality. The idea of CSIS working closely with non-government actors was not envisaged when the *CSIS Act* was passed in 1984. At that time, intelligence activities were focused largely on countering espionage and subversion threats, and did not require the extensive networks that have since been established to counter the global terrorist threat. Thus far, CSIS has managed to work within the existing framework, but SIRC is concerned that these gaps may begin to strain the Service’s operational effectiveness or lead

it to carry out activities that fall outside its mandate.

At the same time, CSIS has been modernizing its traditional investigative techniques to keep pace with new threats. This process was underscored in SIRC’s examination of CSIS’s investigation of cyber threats, which is among the federal government’s intelligence priorities. The review looked at the innovative strategies and tools CSIS is using to move forward with this important

investigation. Similarly, through our review of the Service’s use of the Internet, we gained an appreciation of the way in which this medium supports CSIS’s activities.

SIRC also followed through on its commitment to pay close attention to CSIS’s expanding foreign investigative activities. This year,

we did so by examining a very public issue, CSIS’s role in the interviews of Afghan detainees, within the framework

of its overall operational activity in Afghanistan. SIRC concluded that CSIS should assess and qualify, with care and consistency, information originating from agencies that may engage in human rights abuses—concerns that have animated previous SIRC reviews.

More broadly, we found that the Service’s involvement with the Afghan detainees provides lessons that can be applied

“SIRC has responded to the changing national security environment by looking at CSIS’s operational activities in novel ways, and delving into new lines of inquiry.”

to other operations abroad. Although overseas operations unfold in unique circumstances and present different challenges, CSIS should strive to ensure that the management of its operations abroad mirrors, to the extent practicable, the standards of administration and accountability that are maintained domestically.

This year's review of CSIS's cooperation with a "Five Eyes" partner offered insight into another dimension of the Service's work abroad. SIRC found that the expansion of CSIS activities abroad requires a more integrated approach with its domestic partners. Specifically, we urged CSIS to give further consideration to how it keeps the Department of Foreign Affairs and International Trade—which is ultimately responsible for managing Canada's international relations—regularly apprised of its overseas activities.

Information sharing and cooperation with domestic partners are obviously core components of CSIS's intelligence work, and therefore run through this year's reviews. SIRC looked at one of the Service's most important relationships—with the RCMP—through the lens of one of the intelligence community's most important contemporary challenges: the use of intelligence as evidence. The Committee was left with a positive impression of RCMP–CSIS cooperation, and a strong appreciation of the complexities and challenges of reconciling the need to protect secret intelligence with the need to share it with law enforcement in support of criminal prosecutions.

These findings are only a few highlights of our reviews. Detailed summaries of all the reviews undertaken in the last year are found in the following pages.

Conclusion

Our perspective on a possible future role for SIRC and the results of our reviews are offered here as part of our contribution to a public dialogue on national security. Indeed, Parliament conceived this advisory role for us in 1984 by anticipating that SIRC would play a "vital role in the functioning of the security intelligence system" by promoting "adequate debate, where necessary, in the area of security." Should the government proceed to implement a broader system of independent review for agencies involved in national security, SIRC hopes that its views will assist decision-makers in achieving improvement and in building the confidence of Canadians in their national security apparatus.

SECTION 2:

Summaries of SIRC Reviews and Complaints

A. REVIEWS

SIRC's reviews are designed to provide Parliament and the Canadian public with a broad understanding of the Service's operational activities. In carrying out its reviews, SIRC examines how CSIS has performed its duties and functions to determine if the Service was acting appropriately, effectively and in accordance with the law.

SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and activities. Our research program is designed to address a broad range of subjects on a timely and topical basis.

The difference between oversight and review

Outside Canada, intelligence oversight bodies, such as the select committees of the United States Senate and Congress, examine on a continuous basis the actions of the intelligence agencies. They have the mandate to evaluate current investigations or decisions in "real time," and usually monitor budget and administration, as well. As a result, oversight bodies can be implicated in the decision-making process of intelligence agencies because they have the capacity to influence those decisions as they are being made.

In Canada, by contrast, SIRC reviews past operations of the Service. SIRC is not involved in the day-to-day operational or administrative decisions and activities of the Service, nor is SIRC implicated in those decisions. Reviews give us the distinct advantage of being able to assess fully CSIS's performance, unfettered by any earlier involvement on our part.

In deciding which matters to review, SIRC considers:

- events or developments with the potential to represent threats to the security of Canada;
- intelligence priorities identified by the Government of Canada;
- activities by CSIS that could have an impact on individual rights and freedoms;
- issues identified in the course of SIRC's complaints functions;
- new directions and initiatives announced by or affecting CSIS; and
- the CSIS Director's annual classified report submitted to the Minister of Public Safety.

Each review results in a snapshot of the Service's actions in a specific case. This approach allows SIRC to manage the risk inherent in being able to review only a small number of CSIS activities in any given year.

SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work. As part of this process, researchers may arrange briefings with CSIS employees, as well as examine individual and group targeting files, human source files, intelligence assessments and warrant documents. SIRC can also examine files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources, that may be review-specific. The goal is to look at a diverse pool of

Find out more about SIRC's earlier reviews

Over the years, SIRC has reviewed a wide range of CSIS activities. A complete listing of SIRC's past reviews can be found on our website (www.sirc-csars.gc.ca).

information so that we can ensure that we have thoroughly reviewed and completely understood the issues at hand.

Throughout the years, SIRC has reviewed a wide range of CSIS activities, both domestically and abroad. We have done so by looking at:

- activities undertaken at various CSIS stations around the world;
- activities and investigations of CSIS regional offices;
- CSIS's cooperation and exchanges of information with domestic and foreign partners; and
- specific operational techniques such as CSIS's use of human sources and covert intercepts.

The Committee's reviews include findings and, where appropriate, recommendations. These reviews are forwarded to the Director of CSIS, the Inspector General of CSIS, and Public Safety Canada.

Accountability matters

SIRC is one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through the Minister of Public Safety, the courts, the Inspector General of

CSIS, the central agencies of government (e.g., Privy Council Office, Treasury Board Secretariat), the Auditor General of Canada, the Information Commissioner of Canada and the Privacy Commissioner of Canada.

SIRC's recommendations

Each year, SIRC requests a status report from CSIS on the recommendations arising from the previous year's reviews and complaint decisions. This update gives SIRC the opportunity to track the implementation of our recommendations and to learn about the practical impact of those recommendations on CSIS. This process also allows CSIS to respond formally to SIRC's reviews and decisions, thereby contributing to the ongoing discussion between CSIS and SIRC.

Previously, during the 2009–2010 review period, SIRC made 12 recommendations addressing a wide range of issues. SIRC is pleased to note that CSIS has responded to several of these recommendations. For example, in response to recommendations made in SIRC's review of CSIS's relationships with select domestic front-line partners, CSIS has revamped the primary reporting tool it uses to gauge the status of its domestic relationships, and it is also examining the idea of adding a category in its reporting to indicate when intelligence found in reporting originated from law enforcement partners. Furthermore, in response to SIRC's recommendation that CSIS seek Ministerial guidance on the use of disruption to counter national security threats, CSIS responded that it has brought the issue to the Department of Public Safety for consideration.

SIRC REVIEW:

CSIS's Use of the Internet

Over the span of a generation, information available via the Internet has grown exponentially. Today, it is a vast, interactive medium that offers significant anonymity to people who communicate online.

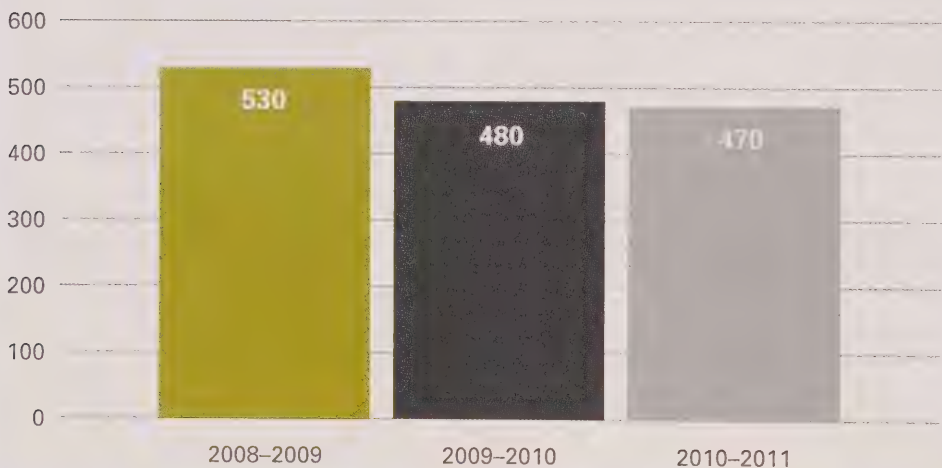
Of particular concern to security intelligence agencies and law enforcement is the growing role that online activities play in the radicalization of individuals who may become threats to Canadian interests. Today, people who may never have met can create networks, mobilize and plan threat-related activities—all without ever having

to leave home. For those who pose a threat to Canada and its allies, online activities play an important role at every stage of radicalization, giving direct access to unfiltered extremist ideology, as well as providing a nearly anonymous meeting place for like-minded radical individuals.

As a result, threat-related online activities have moved to the forefront of many national security investigations. This medium has come to play an important operational role in CSIS investigations: for example, key targets of the "Toronto 18" group were initially detected through the monitoring of material posted online.

Targeting

When the Service has reasonable grounds to suspect that an individual or an organization could pose a threat to Canada, it must first establish an investigation. The figures below indicate the number of targets (rounded to the nearest 10) investigated by CSIS in the past three fiscal years.



SIRC's review

This review examined the strategies, policies and processes that guide CSIS's use of the Internet by focusing on the role of a specialized unit established in 2001. SIRC looked specifically at how this unit's work helps to generate leads and push investigations forward. SIRC's review also looked at the information collected online by the Service.

SIRC's review found that CSIS's use of the Internet has become increasingly common. It is therefore important that the Service have the resources in place to deal with the workload. In that regard, SIRC supports the findings of an internal audit that recognized the importance of addressing these resource issues.

Overall, SIRC found CSIS's approach to its online work to be sound and flexible. SIRC also noted that the Service had developed useful guidelines for certain Internet-based activities. These guidelines incorporate lessons learned and best practices into a useful reference tool.

SIRC identified two issues concerning CSIS's use of the Internet.

First, CSIS's interactions with young Canadians will no doubt increase as extremists continue to use the Internet to attempt to radicalize youth. Indeed, much of the extremist content posted online to recruit and radicalize individuals is targeted at youth—one of the largest groups of

Internet users in Canada and elsewhere. SIRC did not take issue with CSIS collecting information online. However, SIRC believes that the Service needs to give special consideration when dealing with information concerning youth. At issue was the volume of information pertaining to young people being retained by CSIS as part of its operational reporting. SIRC believes that CSIS should impress upon its employees the need to exercise added caution when collecting and retaining information relating to youth.

Second, SIRC underscored the importance of CSIS applying the "strictly necessary" test when collecting and retaining information online. The Internet offers vast amounts of easily accessible information, and care should be taken to ensure that such information is subject to the same "strictly necessary" test as information collected from other sources.

SIRC REVIEW:

CSIS'S Private Sector Relationships

Increased collaboration with non-traditional partners is a growing trend in security intelligence in Canada and elsewhere. Traditionally, CSIS's relationships were with domestic and foreign partners in the public sector, such as domestic police services, other Canadian government departments and agencies, or governments or institutions of foreign states. Today, the Service is also reaching out to non-traditional partners, such as the private sector.

SIRC's review

This review examined CSIS's growing relationship with the private sector in the context of national security. SIRC examined the Service's general liaison and outreach efforts with private sector organizations, which are conducted primarily at the regional level. CSIS has two main programs through which most of these interactions take place:

- the Public Liaison and Outreach Program—briefings intended to sensitize the public sector to CSIS's mandate and to establish CSIS as a point of contact for potentially threat-related information; and
- the Liaison and Awareness Program—more focused briefings on specific threats.

SIRC concluded that CSIS's interactions with the private sector are important and can be helpful when pursuing more specific investigative leads.

SIRC looked at a few instances where CSIS was able to capitalize on private sector relationships. Overall, the Committee found that developing rapport within that milieu is key to CSIS capitalizing on private sector information. In particular, it recognized the efforts of CSIS liaison officers in this regard.

SIRC learned that, in the past, the Service employed a more coordinated and strategic approach with respect to building its private sector relationships. In the interests of leveraging the limited resources available for these activities, and of capitalizing on the experience already gained, **SIRC**

Rules on sharing information regarding security intelligence

The *CSIS Act* prohibits disclosure of information obtained by the Service in the course of its investigations, except in the performance of its duties and functions under the *Act*, or the administration or enforcement of the *Act* or other laws.

Section 19 specifically identifies situations where such sharing of information is permitted:

- disclosures to law enforcement and to officers of the court in an investigation or prosecution;
- disclosures to the Minister of National Defence or of Foreign Affairs, or departmental officials, when the information is relevant to matters relating to Canada's defence or international affairs; or
- disclosures authorized by the Minister of Public Safety that are considered to be in the public interest.

recommended that CSIS expand on the efforts undertaken in regional offices by articulating a Service-wide strategy on managing its relations with the private sector. In SIRC's opinion, an effective strategy would involve identifying those

sectors with the greatest potential to be of investigative value to the Service.

At the same time, there are limitations on CSIS working more closely with the private sector because of the strict laws that govern official information-sharing. The *CSIS Act* does not authorize disclosure of information collected by the Service to non-traditional or non-governmental partners, such as private sector organizations. Section 12 of the *CSIS Act* limits CSIS's responsibility to report to and advise the Government of Canada on national security threats. Although operational policies have been developed to govern information-sharing with the private sector, the policies are appropriately restrictive and provide strict parameters for what information can be shared.

For these reasons, the Service strives to engage and support the private sector's security needs in other ways. For example, it tries to share more unclassified information, namely through its participation in the Integrated Threat Assessment Centre, which produces threat assessments that are distributed to the private sector, among others. Efforts are also underway to increase the number of security clearances for individuals in the private sector, to allow for more meaningful exchanges on issues relating to national security threats.

Finally, CSIS conducts security clearances for the private sector when such requests are sponsored by a federal department or agency, or by an appropriate provincial

authority. Under the Sensitive Site Screening program, for example, CSIS provides clearances for individuals seeking to obtain access to sensitive locations, including nuclear sites, international airports and special events, such as the 2010 Winter Olympics.

SIRC will continue to examine CSIS's relationships with the private sector in future reviews and will pursue, where appropriate, the issues raised in this study to enhance its understanding of the benefits and challenges of the Service's relationships with non-traditional partners.

SIRC REVIEW:

CSIS's Intelligence-to-Evidence Process

Cooperation and information-sharing among members of Canada's security and intelligence community have always been key characteristics of Canada's national security efforts. The relationship between CSIS and the RCMP, in particular, has moved to the forefront following the passage of the *Anti-terrorism Act* (2001). As a result of this legislation, CSIS and the RCMP have had to work more closely together since activities related to terrorism can constitute both a threat to the security of Canada and a crime under the *Criminal Code*.

In the intervening decade, intelligence has been disclosed in a growing number of criminal proceedings—a process that some have called the “judicialization of intelligence” or the “intelligence-to-evidence” process.

In 2008, the Director of CSIS publicly acknowledged that intelligence agencies have had to confront a “range of legal issues such as disclosure, evidentiary standards, and the testimony of intelligence personnel in criminal prosecutions,” all of which have had profound implications for how intelligence work is undertaken and carried out in Canada.

SIRC’s review

SIRC’s review examined how CSIS has responded to the increased use of security intelligence in criminal proceedings. It explored how the Service and the RCMP cooperate while still respecting each other’s roles in counter-terrorism investigations, and what lessons have been learned from recent terrorism prosecutions.

First, SIRC’s review looked at the framework governing cooperation between CSIS and the RCMP, as well as the approaches and tools that the Service—either separately or in conjunction with the RCMP—has developed to manage this important relationship. SIRC found that significant progress had been made in this area. In particular, it found that CSIS and the RCMP have implemented a process that allows for an effective operational partnership.

Next, SIRC took a closer look at how this approach was put to the test during the

Toronto 18 investigation—one of the first major prosecutions under the *Anti-terrorism Act* to have worked its way through the criminal justice system. In SIRC’s view, this case demonstrated CSIS’s ability to work effectively with the RCMP under the new law.

SIRC also examined in detail two judgments rendered by the Ontario Superior Court of Justice in the course of the Toronto 18 trials, focusing on CSIS’s operational coordination and information exchanges with the RCMP. Overall, SIRC found that the Service’s response to both rulings provides useful guidance for future counter-terrorism investigations and prosecutions.

“SIRC found that CSIS and the RCMP have implemented a process that allows for an effective operational partnership.”

Recognizing that discussions concerning intelligence-to-evidence are ongoing, SIRC identified three issues that CSIS may wish to examine more closely.

First, SIRC looked at the two-letter mechanism (i.e., disclosure and advisory letters) currently used by the Service to disclose information to law enforcement. Typically, a disclosure letter is treated as a tip or an investigative lead to initiate or advance a criminal investigation, and is not to be used by police to obtain a warrant. An advisory letter, on the other hand, is the formal means by which CSIS authorizes law enforcement to use its information in applications to the courts to obtain a warrant.

To improve the quality and value of the information that CSIS provides to its law enforcement partners, and to bring consistency to the way in which CSIS discloses information to law enforcement, **SIRC recommended that CSIS adopt a one-letter disclosure model that incorporates the standards of rigorous legal review currently set for advisory letters.**

Second, the importance of cooperation—both early and often—with the RCMP was a recurrent theme. Cooperation in an active investigation entails exchanges at multiple levels, both formal and informal. In its review, SIRC found a gap in the Service's records of daily operational and strategic exchanges with the RCMP. It is important that CSIS keep proper records of verbal exchanges, consistent with recent jurisprudence on the subject of retention, as well as CSIS's own approach to the retention of records.

Third, the Toronto 18 trial demonstrated that the courts in Canada are prepared to challenge the means by which CSIS acquires information disclosed to the RCMP, such as through warrant intercepts. This underscores the importance of ensuring that the principle of full, fair and frank disclosure is entrenched in the CSIS warrant application process. SIRC believes that the obligation to provide full, fair and frank disclosure of all material facts to the courts should be fully understood by all CSIS employees.

The use of security intelligence in criminal proceedings will continue to evolve as CSIS and law enforcement gain more experience in working collaboratively in counter-

terrorism investigations, and as more court decisions provide guidance. Further direction may also come from the federal government: in its December 2010 response to the *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*, the government committed to undertake initiatives to improve the relationship between the use of intelligence and its application as evidence in criminal proceedings. SIRC will continue to examine CSIS's relationship with the RCMP, as it is the Service's most important domestic partner.

SIRC REVIEW:

CSIS's Investigation of Cyber Threats

Post 9/11, Western security intelligence agencies have focused their efforts on countering terrorism. Recently, however, the Director of CSIS stated that Canada is experiencing levels of espionage comparable to the height of the Cold War. Indeed, recent events, such as the discovery of a Russian spy ring operating in the United States in the summer of 2010, serve as a reminder that the threat of espionage is still very real.

Complicating the work of intelligence agencies is the fact that espionage activities have, much like terrorism, changed in nature. Today, individuals, groups and state-sponsored agencies are increasingly using cyberspace to break into government and private sector networks to steal secrets. Accordingly, protecting Canada against cyber threats has become increasingly important to the Government of Canada.

SIRC’s review

This review examined CSIS’s investigation of a cyber threat and, more broadly, how CSIS’s efforts contribute to Canada’s cyber security. First, SIRC examined the nature of the cyber threat in question, as well as some of the key challenges associated with investigating the threat. SIRC then took a closer look at the strategies and tools CSIS was using to move the investigation forward, especially with regards to human source recruitment. Finally, SIRC explored CSIS’s role within a broader “whole-of-government” approach to countering the cyber threat.

SIRC noted that CSIS’s role in investigating cyber threats is limited by its mandate, which is to collect information on threats to the security of Canada and to advise government. To fulfill this goal, CSIS has developed a two-pronged approach to its cyber investigations: first, to seek to attri-

bute cyber attacks against Canada, and second, to determine the motivation behind the attacks.

SIRC’s review found that the migration of espionage threats into the cyber realm has required an expansion of CSIS’s efforts and, over time, the introduction of new methods and powers to use in both the physical and virtual world. For example, CSIS has sought a new range of court-approved warrant powers that are designed to keep pace with the rapidly changing cyber threat environment and, at the same time, to generate investigative leads. SIRC noted that the Service’s new approach appears to have established clear benchmarks for the future success of cyber investigations. In addition, CSIS has tried to optimize operational resources deployed against cyber threats.

CSIS is one of many players that support wider government efforts to mitigate cyber

Warrants

The power to authorize intrusive investigative techniques rests strictly with the Federal Court of Canada. The granting of a warrant provides CSIS with authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telecommunications activities. This table shows the number of Federal Court warrants that were approved in the past three fiscal years.

	2014-15	2015-16	2016-17
New warrants	26	36	55
Replaced or renewed	183	193	176
Total	209[†]	229	231

[†]Included in this number were two urgent warrants.

threats. The largest role falls to Communications Security Establishment Canada (CSEC), which is responsible for protecting the government's computer systems and networks, and for providing it with related mitigation advice. SIRC found that CSIS works very closely with CSEC on cyber incidents, and that their work is complementary. While CSEC's signals intelligence provides CSIS with investigative leads, information collected in the course of CSIS's investigations can enhance CSEC's ability to respond to cyber threats.

Finally, SIRC noted that CSIS conducts briefings with federal government departments and private sector organizations as part of a "whole-of-government" approach to raising awareness of cyber threats. Although this outreach is necessary and within CSIS's investigative duties, targeted outreach efforts hold the potential to develop into activities that could be seen as mitigation. Mitigation, which refers to advice provided to victims, or potential victims, from designated government agencies, does not fall within CSIS's mandate on this file. CSIS's role is consistently outlined as one of support, through its investigative activities, to the government's mitigative efforts which are led by CSEC.

SIRC recognizes that liaison activities are a complement to CSIS's investigative methods, and provide opportunities for CSIS to advance its investigation into cyber threats. However, as CSIS positions itself to keep pace with cyber threats, it should remain focused on its investigative role, and continue to use caution not to engage in activities that could be seen as mitigation.

In fall 2010, the federal government introduced *Canada's Cyber Security Strategy*, which defines the roles and responsibilities of departments and agencies on a range of cyber issues, including cyber-espionage. Given its expertise and mandate, Communications Security Establishment Canada (CSEC) plays a key role. The strategy calls on CSEC to enhance its capacity to detect and discover threats and to respond to cyber threats and attacks against government communications networks and information technology systems. For its part, CSIS is called upon to investigate and advise government on threats to the security of Canada, which includes cyber threats.

SIRC REVIEW:

CSIS's Relationship With a "Five Eyes" Partner

Collaboration with domestic and foreign counterparts is essential for any intelligence agency to fulfill its mandate. This is especially true following the events of 9/11, as intelligence agencies have had to cooperate even more closely to counter a global terrorist threat.

During the Second World War, Britain and the United States worked together closely in intercepting the communications of their enemies—what is commonly known as signals intelligence. In 1946, in the context of the emerging Cold War with the Soviet Union, the two major powers decided to institutionalize this cooperation through a formal agreement. Two years later, Canada joined this alliance, with New Zealand and Australia following suit in 1956. Over the years, the “Five Eyes” has expanded its networks and increased its partnerships with other agencies, leading to greater information-sharing on a variety of state and non-state threats to member countries.

In Canada, CSIS has recognized that the expansion of its investigative activities abroad has led to an unprecedented level of cooperation with foreign partners. Underpinning this collaborative work are the Service’s foreign arrangements, which allow for cooperation and exchanges of information on issues of common concern. CSIS has implemented over 250 foreign arrangements with counterparts around the world; chief among

these are the relationships the Service maintains with what is commonly known as its “Five Eyes” partners.

SIRC’s review

This review examined the history and transformation of the Service’s role within the Five Eyes community by undertaking an in-depth examination of CSIS’s cooperation and exchanges with one Five Eyes partner. SIRC’s review was complemented by a visit to the CSIS foreign station that is responsible for managing these partnerships abroad, and meetings with CSIS’s domestic counterparts at the DFAIT Mission.

The Committee found that, in recent years, changes to the threat environment, fiscal pressures and technological advancements have underscored the importance of collaboration within the Five Eyes community. SIRC also found that CSIS’s expansion of collection activities abroad has led to more information-sharing on targets of mutual concern to the alliance.

The review found a high level of cooperation between CSIS and its Five Eyes partner. Furthermore, cooperation and shared concerns over current issues such as radicalization, the growing use of the Internet and the challenges posed by the growing use of intelligence in criminal proceedings, have contributed to making this country’s security and intelligence agencies key partners for CSIS.

In the course of this review, SIRC identified one issue for CSIS’s consideration as it expands its collection capabilities and activities abroad. SIRC recognizes the

importance of effective interdepartmental communication, especially between CSIS and DFAIT, which is responsible for managing Canada's international relations.

CSIS shares information with DFAIT on a regular basis through several means, ranging from formal disclosures and cooperation at the Headquarters level to direct engagement by CSIS Heads of Station with DFAIT Heads of Mission and/or other DFAIT employees at the Mission. In recent years, the scope of this relationship has expanded with CSIS undertaking more operational activities abroad. In 2005, as CSIS planned to increase its foreign operations, it recognized that a new Memorandum of Understanding (MOU) would have to be struck with DFAIT to help manage issues of mutual interest. The MOU signalled CSIS's recognition that it was a member of a larger Canadian contingent operating abroad, with associated responsibilities.

Yet, SIRC found that there were limited exchanges on CSIS's foreign operational activities with DFAIT, despite the MOU advocating "close cooperation, consultation and coordination" with respect to intelligence activities in Canada and abroad. Building on this observation, **SIRC recommended that CSIS adopt a broader interpretation of its disclosure commitments to DFAIT, to allow the department to prepare itself in the event of an adverse development arising from CSIS's foreign operations.**

SIRC REVIEW:

The Role of CSIS in the Interviews of Afghan Detainees

Within months of 9/11, Canada became involved in a United Nations-led mission to overturn the government of, and stabilize, Afghanistan. One aspect of Canada's involvement in that conflict—the processing of Afghan detainees—has been a flashpoint of public discussion. In 2009, the Canadian public, media and Parliament became aware of CSIS's involvement in the interviewing of detainees in support of Canadian operations in Afghanistan. In recognition of the importance of this file, SIRC announced during an appearance before the Standing Committee on Public Safety and National Security in May 2010 that it would conduct a review of CSIS's involvement in this matter.

CSIS Director Richard Fadden also commissioned an internal study of the Service's participation in the interviews of Afghan detainees, the key findings of which were reported in the media in February 2011. The purpose of the CSIS study was to provide an overview of CSIS's role in this matter: to review its knowledge (or lack thereof) of the abuse/mistreatment of detainees, and to ascertain the legal risk regarding its involvement in these interviews. Overall, SIRC found that CSIS's study achieved its goals, and that the report accurately reflected the nature and extent of CSIS's involvement in Afghanistan. In particular, SIRC's review found no indication

that, in the period during which CSIS conducted detainee interviews, CSIS officers posted to Afghanistan had any first-hand knowledge of the alleged abuse, mistreatment or torture of detainees by Afghan authorities.

SIRC's review

The focus of SIRC's review was broader than the internal CSIS study, and was designed to explore the larger context within which CSIS activities, policy and decision-making evolved with respect to Afghan detainees. SIRC examined the role of the detainee interviews within the framework of the Service's operations in Afghanistan; the nature, utility and effectiveness of CSIS's relationship with its Afghan partners, as well as its exchanges of information with those partners; and finally, any lessons learned that could have a bearing on CSIS's future involvement in these types of overseas operations.

SIRC noted two issues that warranted further consideration: first, the need for CSIS to assess and to qualify, with care and consistency, information originating from agencies that may engage in human rights abuses; and second, the need for CSIS to ensure that the management of its operations abroad mirrors, to the extent that is practicable, the standards of administration and accountability that are maintained domestically.

On the first issue, SIRC found that the information gathered by CSIS's local partners to identify threats to Canada and Canadian operations in Afghanistan was of operational value to the Service. Given ongoing human rights concerns and the possibility that information provided to CSIS could have been derived from torture, it was important that CSIS address this risk by managing its relationship and exchanges of information carefully. One of CSIS's standard risk-mitigation techniques is to use caveats, that is, qualifying statements which accompany information sent from CSIS to a partner agency. SIRC found that it took almost five years after CSIS became involved in Afghanistan for CSIS to caveat these exchanges properly.

*"Overall,
SIRC found that
the Afghan detainee
experience provided
opportunities for CSIS to
enhance its approach to
managing operations
overseas."*

The manner in which CSIS should engage with foreign agencies that may not share Canada's stance on human rights has been outlined in Ministerial Direction, as well as in the 2008 CSIS Deputy Director Operations Directive. SIRC believes that CSIS's Directive makes great strides to promote consistent awareness of the possibility of torture-derived information, and to enhance accountability surrounding the exchange and use of such information. However, the Committee found that the wording of the preamble may leave CSIS vulnerable to potential challenges or criticism regarding its policy on information-sharing with

agencies that have a poor human rights record. As a result, **SIRC recommended that CSIS reword the preamble of the Directive governing exchanges with agencies suspected of human rights abuses, to eliminate any possible misunderstanding.**

The second issue addresses lessons learned for future overseas operations from CSIS's interviews of Afghan detainees. SIRC noted that CSIS did not comprehensively document its role in the interviews of Afghan detainees by keeping records that would confirm the numbers and details of all of the detainee interviews. SIRC believes that, should CSIS continue to expand its activities abroad and to provide support to Canadian efforts in volatile regions of the world, it will need to improve its record management practices in those regions to enhance its own internal accountability.

Along similar lines, SIRC found that, early in CSIS's involvement, there was enough information available on the situation in Afghanistan for the Service to have appreciated the complexity of the environment in which it was operating. As a result, SIRC believes CSIS could have moved more quickly to put in place additional direction or guidelines to promote greater accountability.

Overall, SIRC found that the Afghan detainee experience provided opportunities for CSIS to enhance its approach to managing operations overseas. If CSIS continues to expand its operations abroad, it should take all reasonable measures to ensure that the management of operations meets, as

far as is practicable, the standards of administration and accountability that are maintained domestically. This would include strengthening CSIS's ability to consider the potential implications of those operations prior to undertaking them, and increasingly embracing the notion that, while overseas operations present a different set of challenges, those challenges can be anticipated and planned for and do not have to be conceived as "exceptions" in CSIS's overall strategic planning.

SIRC REVIEW:

How CSIS Evaluates the Reliability of Human Sources

In carrying out its investigations against threats to the security of Canada, CSIS draws upon multiple sources of information, including human sources. Human intelligence is obtained from people who are not professionally trained as intelligence agents, but instead are recruited to provide information to which they have access. Human source operations are extremely sensitive and can be dangerous and difficult. For these reasons, special controls are required to ensure sources' security and safety, as well as to mitigate risks to the Service.

CSIS has long regarded its human source program as the most cost-effective and efficient means of accessing privileged information. Recent successful human source operations reinforce this point: human sources' penetration of, and

reporting on, the Toronto 18 terrorist cell, for example, were instrumental in the successful prosecution of the main conspirators.

SIRC's review

Past SIRC reviews have examined a number of human source issues, but generally with a focus on assessing the degree to which CSIS conducted human source operations in conformity with legislation and operational policy. This review moved beyond these considerations to an assessment of the efficiency and effectiveness of CSIS's human source "validation" process, meaning the way in which CSIS assesses a source's information access, reliability and reporting history to determine the value or weight of information he/she provides.

The validation process is crucial to CSIS's recruitment, development and management of successful human source operations. Accordingly, CSIS officers are guided by various instruments and techniques outlined in the Service's operational policies. To complement this framework, CSIS officers also seek advice from senior investigators and/or managers, as well as from the branch at CSIS HQ that is responsible for providing operational support services, policy guidance and operational security relating to human source issues.

SIRC's review noted that a fast-changing and more complex domestic and international operational environment compelled CSIS to take a closer look at its human source validation process. As a result of this exercise, CSIS identified a need to improve its ability to cope with demographic pressures, employee training and issues related to managerial supervision and mentorship.

Building on CSIS's own observations, the Committee made three recommendations designed to enhance the Service's validation process. **First, SIRC recommended that CSIS develop more rigorous criteria, or seek to establish best practices, with respect to human source validation. Second, CSIS should create a human source "lessons learned" database that is accessible to all intelligence officers to enhance their professional development. Finally, SIRC recommended that CSIS conduct a more systematic method of human source file reviews to help ensure that best practices are being followed and that any findings and/or recommendations are incorporated into the lessons learned database.**

B. COMPLAINTS

In addition to its review function, SIRC conducts investigations into complaints concerning CSIS made by either individuals or groups. The types of complaints that SIRC investigates are described in the *CSIS Act* and can take several forms. Under Section 41 of the *CSIS Act*, SIRC investigates “any act or thing done by the Service”; under Section 42, SIRC investigates complaints about denials of security clearances to federal government employees and contractors. SIRC may also conduct an investigation in relation to referrals from the Canadian Human Rights Commission and Minister’s reports in regards to the *Citizenship Act*.

The complaints process at SIRC

Complaint cases may begin as inquiries to SIRC—either in writing, in person or by phone. Once a written complaint is received, SIRC staff advise a prospective complainant about what the *CSIS Act* requires to initiate a formal complaint.

Once a formal complaint is received in writing, SIRC conducts a preliminary review, which can include any information that might be in the possession of CSIS, except for Cabinet confidences. Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated.

If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more

Committee members, assisted by staff and SIRC’s legal team which will provide legal advice to members on procedural and substantive matters. Pre-hearing conferences may be conducted with the parties to establish and agree on preliminary procedural matters, such as the allegations to be investigated, the format of the hearing, the identity and number of witnesses to be called, the production of documents in advance of the hearing and the date and location of the hearing.

The time to investigate and resolve a complaint will vary in length depending on a number of factors, such as the complexity of the file, the quantity of documents to be examined, the number of hearing days required (both in the presence and the absence of the complainants), and the availability of the participants.

The *CSIS Act* provides that SIRC hearings are to be conducted “in private.” All parties have the right to be represented by counsel and to make representations at the hearing, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to SIRC by any other person. A party may request an *ex parte* hearing (in the absence of the complainant and possibly other parties) to present evidence which, for reasons of national security or other reasons considered valid by SIRC, cannot be disclosed to the other party or their counsel. During such hearings, SIRC’s legal team will

cross-examine the witnesses to ensure that the evidence is appropriately tested and reliable, in order to provide the presiding Member with the most complete and accurate factual information relating to the complaint. Once the *ex parte* portion of the hearing is completed, SIRC will determine whether the substance of the evidence can be disclosed to the excluded parties. If so, SIRC will prepare a summary of the evidence and provide it to the excluded parties once it has been vetted for national security concerns.

When SIRC’s investigation of a complaint made under Section 41 is concluded, it provides a report to the Director of CSIS and to the Minister of Public Safety, as well as a declassified version of the report to the complainant.

On completion of an investigation in relation to a complaint under Section 42 of the *CSIS Act*, SIRC reports its findings and any recommendations to the Minister, the Director of CSIS and the Deputy Head concerned, and provides a declassified version of the report to the complainant.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC’s jurisdiction, or investigated and resolved without a hearing (i.e., via an administrative review).

Table 1
Complaints directed to SIRC

	2013-14	2014-15	2015-16
Carried over	15	22	31
New	30	32	17
Total	45	54	48
Closed†	23	23	32

†Closed files include those where: reports were issued; the Committee did not have jurisdiction; the preliminary conditions of the complaint were not met; or the complaint was discontinued.

How SIRC determines jurisdiction of a complaint...

...under Section 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by “any person” with respect to “any act or thing done by the Service.” Before SIRC investigates, two conditions must be met:

1. The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act*.

...under Section 42

With respect to security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

1. Any person refused federal employment because of the denial of a security clearance;
2. Any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
3. Anyone refused a contract to supply goods or services to the government for the same reason.

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

SIRC INVESTIGATION:

Alleged Improper Conduct by CSIS

SIRC investigated a complaint under Section 41 of the *CSIS Act* in which two complainants alleged that CSIS employees, in attempting to interview one of them, conducted themselves in an inappropriate, harassing and disrespectful manner.

The CSIS employees in question went to the home of one of the complainants on a number of occasions over a period of several days, until they were able to meet with the complainant. SIRC found that the Service had a legitimate interest in interviewing the complainant, and that it was necessary to return to that individual's residence until they were successful in securing an interview.

SIRC determined that questioning by CSIS employees can sometimes appear to be aggressive and pressing without being improper or constituting harassment. In the circumstances of this complaint, SIRC found that the interview conducted by the CSIS employees was within the bounds of propriety and did not constitute harassment.

Further, the two complainants alleged that the CSIS employees minimized the significance of the interview by suggesting that the presence of a lawyer was not required. On this point, SIRC agreed with the Service's position that the presence of a lawyer is not always necessary, especially when conducting preliminary interviews. SIRC also maintained, however, that if an individual wishes to have a lawyer present, those wishes should be respected.

In addition, the complainants alleged that the CSIS employees failed initially to identify themselves properly by indicating only that they were representatives of the federal government. SIRC found that the CSIS employees acted appropriately in this regard. Not identifying themselves to members of the complainant's family as CSIS employees is done, in part, to protect the privacy interests of the complainant.

SIRC also concluded, however, that the CSIS employees could have left a business card, and that this would likely have helped expedite a meeting with the complainant. Similarly, when the complainant indicated that he would not speak to the Service without a lawyer, SIRC found that the reaction

of the CSIS employee—which was to refer the complainants to the phone book for CSIS's general number—was unprofessional.

The final component of the complaint involved an allegation that the conduct of the CSIS employees constituted a violation of the *CSIS Act* as well as Sections 7, 9 and 15 of the *Canadian Charter of Rights and Freedoms*. Although SIRC found certain aspects of the CSIS employees' conduct to have been unreasonable or unprofessional, the evidence did not support a claim that the complainants' rights under the *Charter* were engaged.

SIRC INVESTIGATION:

Alleged Delay in Providing a Security Assessment

SIRC investigated a complaint regarding the alleged delay by the Service in providing its security assessment for a complainant's site access clearance, required for the purpose of employment.

In its investigation, SIRC found that the Service spent over 15 months processing the request for a security assessment, which was eventually cancelled when the complainant was laid off, due to circumstances unrelated to the clearance.

Although SIRC considered that the Service was justified in the steps it took to provide its security assessment, it found that the overall processing time involved in conducting the complainant's security assessment was not reasonable, notwithstanding the

Service's explanation for the delays incurred during the various steps of the process.

CSIS indicated it had made changes in the Security Screening Branch with regard to site access clearances. SIRC was satisfied that this contributed to an improvement to the Service's overall processing time of such clearances. Nevertheless, **SIRC recommended that a tracking system be implemented so that priority can be given to files that fall outside the average processing times.**

SIRC INVESTIGATION:

Alleged Unjust, Unfounded and Unethical Assessment of an Applicant for Permanent Residency

SIRC investigated a complaint concerning advice given by CSIS to Citizenship and Immigration Canada (CIC). The complainant alleged that the Service provided unjust, unfounded and unethical advice to CIC regarding his application for permanent resident status in Canada under the former *Immigration Act*.

SIRC determined that the Service's assessment was not unjust, unfounded or unethical.

SIRC also found the Service interviewer was well-prepared for the complainant's interview and that the resulting report was fully documented and well-balanced.

However, **SIRC recommended that:**

- **the Service identify the facts in support of each of the legislative requirements within a provision when making its assessments, and that it provide its analysis for each of the provisions on which it relies;**
- **the Service not include certain information unless it has been corroborated, and that it include all relevant information when reporting statements made by the subject of the assessment; and**
- **the Service include information that could be relevant to a determination as to whether the admission of an individual to Canada would not be detrimental to the national interest.**

SIRC at a Glance

Committee Membership

SIRC is chaired by the Honourable Arthur T. Porter, P.C., M.D. The other Committee Members are: the Honourable Frances Lankin, P.C.; the Honourable Denis Losier, P.C.; the Honourable Philippe Couillard, P.C., M.D.; and the Honourable Carol Skelton, P.C.

Staffing and Organization

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 20, located in Ottawa. This includes a Deputy Executive Director, a Research Director, a Senior Counsel, a Corporate Services Manager, and other professional and administrative staff.

Committee Members provide staff with direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated to the Executive Director with direction, when necessary, from the Chair as Chief Executive Officer.

As part of their ongoing work, the Chair of SIRC, Committee Members and senior staff participate in regular discussions with the

CSIS executive and staff, and other members of the security intelligence community. These exchanges are supplemented by discussions with academics, security and intelligence experts and other relevant organizations. These activities enrich SIRC's knowledge about issues and debates affecting Canada's national security landscape.

Committee Members and staff also visit CSIS regional offices to understand and assess the day-to-day work of investigators in the field. These visits give SIRC an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. They also provide an opportunity to communicate SIRC's focus and concerns. During the 2010–2011 fiscal year, SIRC visited three regional offices.

With respect to human resources, SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures. Table 2 below presents a breakdown of actual and estimated expenditures.

Table 2

SIRC expenditures 2010–11 (\$ millions)

	2010–11 (Actual)	2010–11 (Approved)
Personnel	2.06	2.05
Goods and Services	1.06	0.64
Total	3.12	2.69

Committee Activities

October 14–15, 2010: Several staff attended a conference of the Canadian Association of Security and Intelligence Studies (CASIS), held in Ottawa.

October 26, 2010: SIRC's Chair gave an interview on CBC Radio One's show, *As it Happens*. An audio copy of the interview is available online at www.cbc.ca/asithappens/episode.

January 21, 2011: SIRC senior staff participated in a bi-annual Review Agencies Forum meeting hosted by the Inspector General of CSIS.

February 2011: The Executive Director, along with representatives from CSIS, the Department of Justice, and Foreign Affairs and International Trade Canada, participated in a capacity-building exercise in Bogotá, Colombia.

February 2011: SIRC's Chair gave an interview to the *Ottawa Citizen* in which he discussed SIRC's role and his views on a number of Canadian intelligence matters.

March 3, 2011: The Committee met with members of the United Kingdom's parliamentary oversight body, the Intelligence and Security Committee.

March 29, 2011: The Chair and Executive Director led a panel discussion entitled "The Challenges of National Security Accountability," organized by the Centre for International Policy Studies at the University of Ottawa. Panelists included: Senator Pamela Wallin, Chair of the Senate Committee on National Security and Defence; Mel Cappe, President of the Institute for Research on Public Policy; Paul Kennedy, former Chair of the RCMP Public Complaints Commission; and Professor Reg Whitaker, distinguished Professor Emeritus at York University. The discussion addressed the democratic challenges inherent in maintaining accountability of the operations of Canada's national security agencies, as well as post-9/11 security practices.

March 31, 2011: The Executive Director participated in a Department of Justice National Security Group training day, presenting an overview for the lawyers present of SIRC's role and functions.

April 10, 2011: SIRC's Chair gave an interview on CBC Radio One's show, *Sunday Edition*. An audio copy of the interview is available online at www.cbc.ca/thesundayedition/shows.

List of SIRC Recommendations

During the 2010–2011 review period, SIRC made the following recommendations stemming from the reviews it conducted, as well as from the complaints it investigated.

CSIS's Private Sector Relationships	In the interests of leveraging limited resources and of capitalizing on the experience already gained, SIRC recommended that CSIS expand on the efforts undertaken in regional offices by articulating a Service-wide strategy on managing its relations with the private sector.
CSIS's Intelligence-to-Evidence Process	To improve the quality and value of the information that CSIS provides to its law enforcement partners, and to bring consistency to the way in which CSIS discloses information to law enforcement, SIRC recommended that CSIS adopt a one-letter disclosure model that incorporates the standards of rigorous legal review currently set for advisory letters.
CSIS's Relationship with a "Five Eyes" Partner	SIRC recommended that CSIS adopt a broader interpretation of its disclosure commitments to DFAIT, to allow the department to prepare itself in the event of an adverse development arising from CSIS's foreign operations.
The Role of CSIS in the Interviews of Afghan Detainees	SIRC recommended that CSIS reword the preamble of its Directive governing exchanges with agencies suspected of human rights abuses to eliminate any possible misunderstanding concerning CSIS's policy on information-sharing with such agencies.
How CSIS Evaluates the Reliability of Human Sources	<p>SIRC recommended that CSIS develop more rigorous criteria, or seek to establish best practices, with respect to human source validation.</p> <p>SIRC recommended that CSIS create a human source "lessons learned" database that is accessible to all intelligence officers to enhance their professional development.</p> <p>SIRC recommended that CSIS conduct a more systematic method of human source file reviews to help ensure that best practices are being followed and that any findings and/or recommendations are incorporated into the lessons learned database.</p>

**Alleged Delay in
Providing a Security
Assessment**

SIRC recommended that a tracking system be implemented within CSIS's security assessment process so that priority can be given to files that fall outside the average processing times.

**Alleged Unjust,
Unfounded and
Unethical Assessment
of an Applicant for
Permanent Residency**

SIRC recommended that CSIS identify the facts in support of each of the legislative requirements within a provision when making its assessments, and that it provide its analysis for each of the provisions on which it relies.

SIRC recommended that CSIS not include certain information unless it has been corroborated, and that it include all relevant information when reporting statements made by the subject of the assessment.

SIRC recommended that CSIS include information that could be relevant to a determination as to whether the admission of an individual to Canada would not be detrimental to the national interest.

Retard présumé à fournir une évaluation de sécurité

Le CSARS a recommandé que le processus d'évaluation de sécurité du SCRS soit assorti d'un système de repérage permettant de donner priorité aux dossiers dont le temps de traitement dépasse la moyenne.

Évaluation présumée injuste, sans fondement et contraire à l'éthique, d'un demandeur de résidence permanente

Le CSARS a recommandé que le SCRS identifie les faits à l'appui de chacune des exigences de la loi contenues dans une disposition, lorsqu'il fait ses évaluations, et qu'il présente son analyse pour chaque disposition sur laquelle il se fonde.

Le CSARS a recommandé que le SCRS n'inclue pas certaines informations, sauf si elles ont été corroborées, et qu'il inclue toutes celles qui sont pertinentes lorsqu'il fait état de déclarations du sujet de l'évaluation.

Le CSARS a recommandé que le SCRS inclue l'information qui pourrait être pertinente à une décision quant à savoir si l'admission d'un individu au Canada ne serait nullement préjudiciable à l'intérêt national.

Liste des recommandations du CSARS

Au cours de la période à l'étude 2010-2011, le CSARS a formulé les recommandations suivantes, qui découlent de ses études ainsi que des plaintes sur lesquelles il a enquêté.

Les relations du CSARS avec le secteur privé	<p>Dans le but d'optimiser les ressources limitées dont on dispose et de tirer parti de l'expérience acquise, le CSARS a recommandé que le SCRS multiplie les efforts entrepris dans les bureaux régionaux en élaborant à l'échelle du Service une stratégie pour la gestion de ses relations avec le secteur privé.</p> <p>Pour améliorer la qualité et la valeur des informations fournies par le SCRS à ses partenaires de l'application de la loi et rendre cohérente la manière dont il les leur communique, le CSARS a recommandé que le SCRS adopte un modèle de communication qui comporte une seule note intégrant les normes d'examen juridique rigoureux fixées actuellement pour les notes d'instructions.</p>
Le processus de transformation en preuves des informations du SCRS	<p>Pour améliorer la qualité et la valeur des informations fournies par le SCRS à ses partenaires de l'application de la loi et rendre cohérente la manière dont il les leur communique, le CSARS a recommandé que le SCRS adopte un modèle de communication qui comporte une seule note intégrant les normes d'examen juridique rigoureux fixées actuellement pour les notes d'instructions.</p>
La relation du SCRS avec un partenaire des « Five Eyes »	<p>Le CSARS a recommandé que le SCRS adopte une interprétation plus large de son engagement à communiquer des renseignements au MAECI afin de permettre à celui-ci de se préparer à tout effet négatif qui pourrait découler d'opérations du Service à l'étranger.</p>
Le rôle du SCRS dans les entrevues de détenus afghans	<p>Le CSARS a recommandé que le SCRS reformule le préambule de la directive, concernant les échanges avec des services soupçonnés d'avoir de mauvais antécédents en matière de respect des droits de la personne, afin d'éviter toute méprise possible concernant la politique du SCRS sur l'échange d'informations avec ces services.</p>
La méthode d'évaluation de la fiabilité des sources humaines par le SCRS	<p>Le CSARS a recommandé que le SCRS élabore des critères plus rigoureux, ou cherche à instaurer des pratiques exemplaires, en ce qui touche la validation des sources humaines.</p> <p>Le CSARS a recommandé que le SCRS crée une base de données qui regroupe « les leçons tirées » et qui soit accessible à tous les agents de renseignement afin d'améliorer le perfectionnement professionnel.</p> <p>Le CSARS a recommandé que le SCRS recoure à une méthode plus systématique d'étude des dossiers de sources humaines afin de contribuer à assurer la conformité aux pratiques exemplaires et l'intégration de toute constatation et/ou recommandation dans la base de données sur les leçons tirées.</p>

Tableau 2
Dépenses du CSARS 2010-2011 (en millions de dollars)

Personnel	2,06	2,05
Biens et services	1,06	0,64
Total	3,12	2,69

26 octobre 2010 : Le président du CSARS a été interviewé à l'émission « As it Happens » de CBC Radio One. L'enregistrement de l'entrevue est disponible en ligne (en anglais seulement) à cette adresse : www.cbc.ca/asithappens/episode.

21 janvier 2011 : Les cadres supérieurs du CSARS ont participé à une réunion semestrielle du Forum des organismes de surveillance, tenue par l'inspecteur général du SCRS.

Février 2011 : La directrice exécutive, accompagnée de représentants du SCRS, du ministère de la Justice ainsi que d'Affaires étrangères et Commerce international Canada, a participé à un exercice de renforcement de capacité à Bogotà, en Colombie.

Février 2011 : Le président du CSARS a accordé au *Ottawa Citizen* une entrevue au cours de laquelle il a discuté du rôle du Comité et exposé ses opinions sur diverses questions concernant le renseignement canadien.

3 mars 2011 : Les membres du CSARS ont rencontré leurs homologues de l'organisme de contrôle parlementaire du Royaume-Uni, appelé Intelligence and Security Committee.

29 mars 2011 : Le président et la directrice exécutive ont dirigé un débat d'experts

intitulé « The Challenges of National Security Accountability », organisé par le Centre d'études en politiques internationales à l'Université d'Ottawa. Au nombre des experts figuraient la sénatrice Pamela Wallin, présidente du Comité sénatorial de la sécurité nationale et de la défense; Mel Cappe, président de l'Institut de recherche en politiques publiques; Paul Kennedy, ancien président de la Commission des plaintes du public contre la GRC; et le professeur émérite Reg Whitaker, de l'Université York. Les participants au débat se sont penchés sur les défis inhérents d'ordre démocratique qu'il faut relever pour assurer la reddition de comptes relative aux opérations des organismes qui s'occupent de la sécurité nationale au Canada, et sur les pratiques de sécurité depuis les attaques du 11 septembre.

31 mars 2011 : La directrice exécutive a participé à une journée de formation tenue par le Groupe de la sécurité nationale du ministère de la Justice, donnant un aperçu du rôle et des fonctions du CSARS à l'intention des avocats présents.

10 avril 2011 : Le président du CSARS a accordé une entrevue à l'émission « Sunday Edition » de CBC Radio One. L'enregistrement de l'entrevue est disponible en ligne (en anglais seulement) à cette adresse : www.cbc.ca/thesundayedition/shows.

Surviv du CSARS

Composition du Comité

La présidence du CSARS est occupée par l'honorable Arthur T. Porter, C.P., M.D. Les autres membres du Comité sont l'honorable Frances Lankin, C.P., l'honorable Denis Losier, C.P., l'honorable Philippe Couillard, C.P., M.D., et l'honorable Carol Skelton, C.P.

Personnel et organisation

Le CSARS jouit du soutien d'une directrice exécutive, Susan Pollak, et d'un effectif autorisé de 20 employés, en poste à Ottawa. Cet effectif comprend un sous-directeur exécutif, un directeur de la recherche, un avocat principal, un directeur des services généraux et d'autres professionnels et agents administratifs.

Les membres du Comité dictent au personnel l'orientation à donner aux travaux de recherche et autres activités désignées prioritaires pour l'année. La marche des affaires courantes est confiée à la directrice exécutive qui s'enquiert au besoin de la ligne de conduite à tenir auprès du président, en sa qualité de premier dirigeant du CSARS. Dans le cadre de leurs travaux suivis, le président et les membres ainsi que les cadres supérieurs du Comité prennent part à des discussions régulières avec la direction et le personnel du SCRS et avec d'autres membres de la collectivité du renseignement de sécurité. À ces échanges se greffent des discussions avec des universitaires et des experts du renseignement et de la

sécurité et avec d'autres organismes compétents. Ces activités enrichissent les

connaissances du CSARS au sujet des questions et débats qui entourent le paysage de la sécurité nationale au Canada.

Les membres et les cadres du Comité visitent aussi les bureaux régionaux du

SCRS afin de comprendre et d'évaluer le travail courant des enquêteurs locaux. Ces visites leur fournissent l'occasion de se faire

exposer les problèmes, difficultés et priorités propres à ces bureaux par les cadres régionaux du Service. Elles leur permettent

aussi de faire valoir ce qui polarise les efforts et les préoccupations du CSARS. Au cours de l'exercice 2010-2011, les mem-

bres du CSARS se sont rendus dans trois bureaux régionaux.

Au chapitre des ressources humaines, le CSARS continue de gérer ses activités

dans les limites des ressources qui lui sont octroyées. Ses principales dépenses ont

trait au traitement de son personnel et à ses déplacements afin de participer aux audiences, aux exposés et aux activités

de surveillance du Comité au Canada. Le tableau 2 présente une ventilation des dépenses réelles et des prévisions

de dépenses.

Activités du Comité

14-15 octobre 2010 : Plusieurs cadres ont pris part à une conférence tenue à Ottawa par l'Association canadienne pour les études de renseignement et de sécurité.

que le temps global qu'il lui a fallu pour effectuer l'évaluation de sécurité du plaigant n'était pas raisonnable, en dépit des motifs avancés par le Service pour expliquer les retards attribuables aux diverses étapes du processus.

Le SCRS a indiqué qu'il avait effectué des changements à la Direction du filtrage de sécurité en ce qui concerne les autorisations d'accès à des sites. Le CSARS est convaincu que ces changements ont contribué à améliorer le temps de traitement global de ces demandes d'autorisation au Service. Néanmoins, le CSARS a recommandé que soit mis en œuvre un système de repérage permettant de donner priorité aux dossiers dont le temps de traitement dépasse la moyenne.

ENQUÊTE DU CSARS : Évaluation présumée injuste, sans fondement et contraire à l'éthique, d'un demandeur de résidence permanente

Le CSARS a enquêté sur une plainte concernant des conseils donnés par le SCRS à Citoyenneté et Immigration Canada (CIC). Le plaigant a allégué que le Service avait fourni à CIC des conseils injustes, sans fondement et contraires à l'éthique concernant sa demande de statut de résident permanent au Canada en vertu de l'ancienne Loi sur l'immigration.

Le CSARS a déterminé que l'évaluation du Service n'était pas injuste, sans fondement ou contraire à l'éthique. Il a aussi constaté que l'intervieweur du Service était bien préparé pour l'entrevue du plaigant et que le rapport d'entrevue était pleinement documenté et bien équilibré.

Cependant, le CSARS a recommandé que :

- le Service identifie les faits à l'appui de chacune des exigences de la loi contenues dans une disposition, lorsqu'il fait ses évaluations, et qu'il présente son analyse pour chaque disposition sur laquelle il se fonde; le Service n'inclue pas certaines informations, sauf si elles ont été corroborées, et qu'il inclue toutes celles qui sont pertinentes lorsqu'il fait état de déclarations du sujet de l'évaluation;
- le Service inclue l'information qui pourrait être pertinente à une décision quant à savoir si l'admission d'un individu au Canada ne serait nullement préjudiciable à l'intérêt national.

plaignant. De même, le CSARS a constaté que, lorsque le plaignant a affirmé qu'il ne parlerait pas au Service sans la présence d'un avocat, l'employé du SCRS a eu une réaction peu professionnelle – invitant les plaignants à chercher le numéro général du SCRS dans l'annuaire téléphonique.

Le dernier élément de la plainte comportait l'allégation que le comportement des employés du SCRS violait la *Loi sur le SCRS* et les articles 7, 9 et 15 de la *Charte canadienne des droits et libertés*. Même si le CSARS a constaté que certains aspects du comportement des employés du SCRS n'étaient ni raisonnables ni professionnels, la preuve ne permet pas de conclure que les droits des plaignants reconnus par la *Charte* étaient en cause.

ENQUÊTE DU CSARS :

Retard présumé à fournir

une évaluation de sécurité

Le CSARS a enquêté sur une plainte relative au retard du Service à fournir une évaluation de sécurité qui visait à autoriser le plaignant à accéder à des sites particuliers et dont il avait besoin pour être embauché. Dans son enquête, le CSARS a constaté que le Service avait mis plus de 15 mois à traiter la demande d'évaluation de sécurité, qui a finalement été annulée quand le plaignant a été licencié en raison de circonstances étrangères à l'autorisation. Le CSARS estime que les étapes franchies par le Service pour fournir son évaluation de sécurité étaient justifiées, mais il a constaté

employés devaient retourner à la résidence de l'intéressé tant qu'ils ne pourraient pas obtenir une entrevue.

Le CSARS a déterminé qu'un interrogatoire mené par des employés du SCRS peut parfois sembler agressif et pressant, sans être inadéquat ou constituer du harcèlement. Dans les circonstances de cette plainte, le CSARS a constaté que l'entrevue menée par les employés du SCRS respectait les convenances et ne constituait pas du harcèlement.

De plus, les deux plaignants ont allégué que les employés du SCRS avaient minimisé l'importance de l'entrevue en affirmant que la présence d'un avocat n'était pas nécessaire. Sur ce point, le CSARS est d'accord avec la position du Service voulant que la présence d'un avocat ne soit pas toujours nécessaire, notamment lors d'entrevues préliminaires. Cependant, le CSARS a aussi soutenu que, si une personne souhaite la présence d'un avocat, ce souhait devrait être respecté.

De surcroît, les plaignants ont allégué que les employés du SCRS avaient négligé au départ de s'identifier comme il fallait, se disant seulement des représentants du gouvernement fédéral. Le CSARS a constaté que ces employés avaient agi de manière irréprochable à cet égard. S'ils ne se présentent pas comme des employés du Service aux membres de la famille du plaignant, c'est entre autres pour protéger sa vie privée. Le CSARS a aussi conclu, toutefois, que les employés du SCRS auraient pu laisser une carte professionnelle et que cela aurait probablement hâté la rencontre avec le

Détermination de la compétence du CSARS à examiner une plainte...

...en vertu de l'article 41

En vertu de l'article 41 de la *Loi sur le*

SCRS, le CSARS est tenu de faire

enquête sur les plaintes que « toute

personne » peut porter « contre des

activités du Service ». Pour que le

CSARS fasse enquête, deux condi-

tions doivent être remplies :

1. le plaignant doit d'abord avoir présenté sa plainte par écrit au directeur du SCRS sans recevoir de réponse dans un délai raisonnable (environ 30 jours) ou, s'il en a reçu une, sans que cette réponse le satisfasse;

2. le CSARS doit être convaincu que la plainte n'est pas frivole, vexatoire ou sans objet, ni entachée de mauvaise foi.

Le CSARS ne peut enquêter sur une

plainte qui peut être réglée autrement,

par une procédure de griefs en vertu

de la *Loi sur le SCRS* ou de la *Loi*

sur les relations de travail dans

la fonction publique.

...en vertu de l'article 42

Quant aux habilitations de sécurité, le

CSARS est tenu, selon l'article 42 de la

Loi sur le SCRS, de faire enquête sur

les plaintes présentées par :

1. les personnes qui ne sont pas embauchées par le gouvernement fédéral à cause du refus d'une habilitation de sécurité;

2. les fonctionnaires fédéraux qui sont renvoyés, rétrogradés ou mutés ou qui se voient refuser une mutation ou une promotion pour la même raison;
3. les personnes qui se voient refuser un contrat pour la fourniture de biens ou de services au gouvernement, toujours pour le même motif.

Les plaintes semblables doivent être

présentées dans les 30 jours du refus

de l'habilitation de sécurité. Le CSARS

peut prolonger cette période si des

raisons valables lui sont fournies.

Enquête du CSARS :

Présumé comportement

inadéquat de la part du SCRS

Le CSARS a enquêté sur une plainte, rele-

vant de l'article 41 de la *Loi sur le SCRS*, dont

les deux auteurs prétaient un comportement

inadéquat, harcelant et irrespectueux à des

employés du SCRS qui avaient tenté

d'interviewer l'un d'eux.

Les employés en cause sont allés au domi-

cile d'un des plaignants à diverses reprises

en une période de plusieurs jours, jusqu'à ce

qu'ils réussissent à le rencontrer. Le CSARS

a constaté que le Service avait un intérêt

légitime à interviewer le plaignant et que ses

Tableau 1
Plaintes présentées au CSARS

Reportées de l'exercice précédent	15	22	31
Nouvelles	30	32	17
Total	45	54	48
Dossiers réglés ¹	23	23	32

¹ Les dossiers réglés comprennent les plaintes qui ont donné lieu à un rapport, que le Comité a jugées hors de sa compétence, ou encore qui ne remplissaient pas les conditions préliminaires ou ont été abandonnées.

observations au CSARS, ni y avoir accès ou les commenter. Une partie peut demander une audience *ex parte* (en l'absence du plaignant et, peut-être, d'autres parties) au cours de laquelle elle présente des preuves qui, pour des raisons de sécurité nationale ou pour d'autres motifs jugés valables par le CSARS, ne peuvent être révélées à l'autre partie ou à son avocat. Lors d'une telle audience, l'équipe de juristes du CSARS contre-interroge les témoins pour s'assurer que les preuves ont été bien vérifiées et sont fiables, de manière à fournir au membre-président du CSARS, au sujet de la plainte, de l'information complète et exacte. Une fois terminé le volet *ex parte* de l'audience, le CSARS détermine si la substance de la preuve peut être dévoilée aux parties exclues. Le cas échéant, il prépare un résumé de la preuve et le leur présente, une fois celui-ci expurgé pour des raisons de sécurité nationale.

Une fois que le CSARS a terminé son enquête sur une plainte relevant de l'article 41 de la Loi sur le SCRS, il présente un rapport au directeur du SCRS et au ministre de la Sécurité publique ainsi qu'une version déclassifiée du rapport au plaignant. À l'issue d'une enquête relative à une plainte en vertu de l'article 42 de la Loi, le CSARS fait rapport de ses conclusions et de toute recommandation au ministre, au directeur du SCRS et à l'administrateur général concerné, et il présente une version déclassifiée du rapport au plaignant. Le tableau 1 expose l'état des diverses plaintes qui ont été présentées au CSARS au cours des trois derniers exercices financiers, y compris celles qui lui ont été adressées à tort, qui étaient hors de sa compétence ou qui ont été réglées à la suite d'une enquête sans nécessiter d'audience (p. ex. par un examen administratif).

Outre sa fonction de surveillance, le CSARS est investi de celle d'enquêter sur les plaintes présentées par des personnes ou des groupes à l'endroit du SCRS. Les types de plaintes visées par ses enquêtes sont décrits dans la *Loi sur le SCRS* et prennent diverses formes. En vertu de l'article 41 de cette loi, le CSARS enquête sur les plaintes qui concernent « des activités du Service » et, selon l'article 42, sur celles qui ont trait au refus d'habilitations de sécurité à des fonctionnaires ou à des fournisseurs du gouvernement fédéral. Le CSARS peut aussi faire enquête sur les renvois de la Commission canadienne des droits de la personne et sur les rapports du ministre concernant la *Loi sur la citoyenneté*.

Le processus relatif aux plaintes au CSARS

La première étape d'un dossier de plainte peut être la présentation d'une demande de renseignements au Comité, soit par écrit, en personne ou par téléphone. Sur réception d'une plainte écrite, le personnel du CSARS informe le plaignant éventuel des exigences de la *Loi sur le SCRS*, pour qu'un dossier de plainte officiel puisse être ouvert.

Lorsqu'il reçoit une plainte officielle par écrit, le CSARS effectue un examen préliminaire qui peut porter sur toute information que pourrait détenir le SCRS, à l'exception des documents confidentiels du Cabinet. Si la plainte ne satisfait pas à certaines exigences de la loi, le CSARS la déclare hors

de sa compétence et n'ouvre pas d'enquête à ce sujet.

Si le CSARS détermine qu'il a compétence, il enquête sur la plainte lors d'une audience quasi judiciaire présidée par un ou plusieurs de ses membres, secondés par son personnel et par son équipe de juristes qui leur fournit des avis concernant la procédure et les questions de fond. Des conférences préparatoires peuvent être tenues avec les parties, avant l'audience, pour établir et régler les questions préliminaires de procédure, comme les allégations sur lesquelles faire enquête, le type d'audience, l'identité et le nombre de témoins à citer, les documents à produire en vue de l'audience ainsi que la date et l'endroit de celle-ci.

Le temps nécessaire à l'enquête et au règlement d'une plainte peut varier d'après divers facteurs, dont la complexité du dossier, la quantité de documents à examiner, le nombre de jours d'audience requis (tant en présence des plaignants qu'en leur absence) et la disponibilité des participants.

Selon la *Loi sur le SCRS*, les audiences du CSARS doivent être tenues « en secret ». Chacune des parties a le droit d'être représentée par un avocat et de formuler des observations à l'audience, mais aucune ne peut, de plein droit, être présente au moment où une autre personne expose ses

Le processus de validation est essentiel au SCRS pour les besoins du recrutement ainsi que de la mise sur pied et de la gestion d'opérations fructueuses faisant appel à des sources humaines. En conséquence, ses agents se fondent sur divers instruments et techniques qui sont décrits dans sa politique opérationnelle. Pour compléter ce cadre, ils demandent aussi conseil à des enquêteurs et/ou à des gestionnaires supérieurs ainsi qu'à la Direction des sources humaines et du soutien aux opérations qui, à l'Administration centrale du SCRS, a charge de fournir des services de soutien opérationnel et des orientations en matière de politique et d'assurer la sécurité opérationnelle relative aux questions touchant les sources humaines.

Dans son étude, le CSARS mentionne qu'un cadre opérationnel plus complexe et évoluant rapidement, à la fois au Canada et à l'étranger, a forcé le SCRS à étudier de plus près son processus de validation des sources humaines. Cet examen a permis au SCRS de prendre conscience de la nécessité d'améliorer sa capacité à faire face aux pressions démographiques, à la formation

des employés et aux questions touchant la supervision et le mentorat par des cadres. Fort des observations du SCRS même, le Comité a formulé trois recommandations visant à améliorer le processus de validation du Service. Premièrement, le CSARS a recommandé que le SCRS élabore des critères plus rigoureux, ou cherche à instaurer des pratiques exemplaires, en ce qui touche la validation des sources humaines. Deuxièmement, le SCRS devrait créer une base de données qui regroupe les leçons tirées en matière de sources humaines et qui soit accessible à tous les agents de renseignement afin d'améliorer le perfectionnement professionnel. Enfin, le CSARS a recommandé que le SCRS recoure à une méthode plus systématique d'étude des dossiers de sources humaines afin de contribuer à assurer la conformité aux pratiques exemplaires et l'intégration de toute constatation et/ou recommandation dans la base de données sur les leçons tirées.

provient de gens qui n'ont pas de formation professionnelle à titre d'agents de renseignement, mais qui sont plutôt recrutés pour fournir les renseignements auxquels ils ont accès. Les opérations faisant appel à des sources humaines sont extrêmement délicates et peuvent être dangereuses et difficiles. Pour ces motifs, il faut des moyens de contrôle spéciaux afin d'assurer la sécurité et la sûreté des sources et d'atténuer les risques que court le Service.

Le SCRS considère depuis longtemps son programme de sources humaines comme le moyen le plus rentable et efficace d'obtenir des informations privilégiées. De fructueuses opérations ayant récemment fait appel à des sources humaines renforcent cet argument. Ainsi, la pénétration par des sources humaines, de la cellule terroriste du « groupe des 18 de Toronto », et les rapports la concernant ont joué un rôle-clé dans la poursuite fructueuse des principaux conspirateurs.

Étude du CSARS

Dans de précédentes études, le CSARS a examiné diverses questions concernant les sources humaines, mais il s'attachait généralement alors à évaluer dans quelle mesure le SCRS menait les opérations faisant appel à de telles sources dans le respect de la loi et de la politique opérationnelle. La présente étude déborde ces considérations et évalue l'efficacité et l'efficacité du processus de « validation » des sources humaines par le SCRS, soit la manière dont celui-ci juge l'accès d'une source à des informations, sa fiabilité et l'historique de ses rapports, afin de déterminer la valeur ou le poids des renseignements qu'elle fournit.

Dans le même ordre d'idées, le CSARS a constaté qu'au début de la participation du SCRS, on disposait de suffisamment d'informations sur la situation en Afghanistan pour que celui-ci puisse évaluer la complexité du milieu dans lequel il menait ses opérations. En conséquence, le CSARS est d'avis que le SCRS aurait pu instaurer plus rapidement des orientations ou lignes directrices supplémentaires propres à promouvoir une reddition de comptes plus serrée.

Globalement, le CSARS a constaté que l'expérience relative aux détenus afghans avait fourni au SCRS des occasions d'améliorer son approche à la gestion des opérations menées à l'étranger. Si le Service continue d'intensifier ces opérations, il devrait prendre toutes les mesures raisonnables pour assurer que leur gestion respecte les normes d'administration et de reddition de comptes observées au Canada, autant que faire se peut. Cela consisterait, entre autres, à renforcer la capacité du SCRS à peser les incidences possibles de ces opérations, avant de les entreprendre, et à adhérer de plus en plus à l'idée que, même si les opérations à l'étranger suscitent une gamme différente de défis, on peut entrevoir ces défis et planifier en conséquence et il n'est pas nécessaire d'en faire des « exceptions » dans la planification stratégique globale du SCRS.

ÉTUDE DU CSARS :

La méthode d'évaluation de la fiabilité des sources humaines par le SCRS

Dans ses enquêtes sur les menaces contre la sécurité du Canada, le SCRS puise à diverses sources d'informations, dont les sources humaines. Le renseignement humain

la reddition de comptes entourant l'échange et l'utilisation de ces informations. Cependant, le Comité a constaté que la formulation du préambule de la directive peut exposer le SCRS à des difficultés ou critiques possibles concernant sa politique sur l'échange d'informations avec des services qui ont de mauvais antécédents en matière de respect des droits de la personne, afin d'éviter toute méprise possible. La deuxième la question a trait aux leçons tirées des entrevues de détenus afghans par le SCRS, pour les opérations qui seront menées à l'étranger dans l'avenir. Le CSARS a noté que le Service ne documentait pas complètement son rôle dans les entrevues de détenus afghans en tenant des dossiers confirmant à la fois le nombre d'entrevues et les détails de chacune. Le CSARS estime que, si le SCRS continue d'intensifier ses activités à l'étranger et de soutenir les efforts déployés par le Canada dans les régions explosives du globe, le Service devra peaufiner ses pratiques de gestion de dossiers dans ces régions afin d'améliorer sa propre reddition de comptes interne.

réunies par les partenaires locaux du SCRS, et les opérations du Canada en Afghanistan, étaient précieuses pour le Service sur le plan opérationnel. Compte tenu des craintes constantes en matière de respect des droits de la personne et de la possibilité que des informations fournies au SCRS aient pu être obtenues au moyen de la torture, il importait que celui-ci cherche à atténuer ces risques en gérant avec soin ses relations et ses échanges d'informations. L'un des moyens courants employés par le Service pour atténuer les risques est d'accompagner de réserves, c'est-à-dire d'énoncés descriptifs, les informations qu'il fournit à un service partenaire. Le CSARS a constaté qu'il avait fallu près de cinq ans au SCRS, après son intervention en Afghanistan, pour joindre à ces échanges les réserves qu'il fallait. Tout comme le sous-directeur des Opérations du SCRS l'avait fait en 2008 dans une nouvelle directive, le Ministre a souligné que le SCRS devrait prendre auprès des services étrangers qui n'ont peut-être pas la même position que le Canada en matière de droits de la personne. Le CSARS estime que la directive du SCRS est un grand pas pour ce qui est d'inviter à être constamment aux aguets du risque que des informations soient obtenues sous la torture et à améliorer

« Globalement, le CSARS a constaté que l'expérience relative aux détenus afghans avait fourni au SCRS des occasions d'améliorer son approche à la gestion des opérations menées à l'étranger. »

recommandé que le SCRS reformule le préambule de la directive, concernant les échanges avec des services soupçonnés d'avoir de mauvais antécédents en matière de respect des droits de la personne, afin d'éviter toute méprise possible.

ÉTUDE DU CSARS :

Le rôle du SCRS dans les entrevues

de détenus afghans

Dans les mois qui ont suivi le 11 septembre, le Canada a pris part à une mission dirigée par l'Organisation des Nations Unies et visant à renverser le gouvernement de l'Afghanistan et à stabiliser ce pays. L'un des aspects de sa participation à ce conflit, le traitement de détenus afghans, a littéralement enflammé le débat public. En 2009, la population, les médias et le Parlement du Canada ont appris le rôle joué par le SCRS dans les entrevues de détenus destinées à appuyer les opérations canadiennes en Afghanistan. Compte tenu de l'importance de ce dossier, le CSARS a annoncé, lors de sa comparution devant le Comité permanent de la sécurité publique et nationale en mai 2010, qu'il effectuerait une étude sur le rôle joué par le SCRS dans cette affaire.

Le directeur du SCRS, Richard Fadden, a aussi commandé, sur la participation du Service aux entrevues de détenus afghans, une étude interne dont les principales constatations ont fait l'objet de reportages médiatiques en février 2011. L'objectif de cette étude était de donner une vue d'ensemble du rôle du SCRS dans cette affaire : examiner ce qu'il savait (ou ignorait) des mauvais traitements infligés aux détenus et jauger le risque juridique auquel sa participation à ces entrevues l'exposait. Globalement, le CSARS a constaté que l'étude du SCRS avait atteint ses objectifs et que le rapport traduisait avec exactitude la nature et l'ampleur de son rôle en Afghanistan. L'étude du CSARS n'a notamment

Étude du CSARS

Le champ de l'étude du CSARS était plus vaste que celui de l'étude interne du SCRS et visait à explorer le contexte plus large dans lequel les activités, la politique et la prise de décisions du SCRS ont évolué relativement aux détenus afghans. Le CSARS a examiné le rôle des entrevues de détenus dans le cadre des opérations du Service en Afghanistan; la nature, l'utilité et l'efficacité des relations du SCRS avec ses partenaires afghans ainsi que ses échanges d'informations avec eux; et, enfin, toutes les leçons tirées qui pourraient avoir une incidence sur la participation future du SCRS à de semblables opérations à l'étranger.

Le CSARS a fait état de deux questions justifiant une étude plus poussée : premièrement, la nécessité que le SCRS évalue avec soin et cohérence, en les assortissant de réserves, les informations émanant de services susceptibles de transgresser les droits de la personne, et deuxièmement, la nécessité que le SCRS s'emploie à veiller à ce que la gestion de ses opérations à l'étranger soit la plus conforme possible aux normes d'administration et de reddition de comptes qui sont observées au Canada.

En ce qui touche la première question, le CSARS a constaté que les informations

entre le SCRS et le MAECI, qui a charge de gérer les relations internationales du Canada.

Le SCRS échange des renseignements régulièrement avec le MAECI par divers moyens qui vont de communications officielles à la coopération au niveau de l'Administration centrale en passant par un engagement direct des chefs de poste du SCRS auprès des chefs de mission et/ou des autres employés du MAECI dans les missions. Depuis quelques années, cette relation a pris de l'ampleur du fait que le SCRS a intensifié ses activités opérationnelles à l'étranger. En effet, en 2005, au moment où il planifiait cette intensification, le SCRS a reconnu qu'il devait conclure un nouveau protocole d'entente avec le MAECI pour faciliter la gestion des questions d'intérêt mutuel. Ce protocole fait état de l'appartenance du SCRS, assortie de responsabilités connexes, à un vaste contingent canadien œuvrant à l'étranger.

Pourtant, le CSARS a constaté que les échanges avec le MAECI concernant les activités opérationnelles du SCRS à l'étranger étaient limités, en dépit du fait que, dans le protocole, on préconise « une coopération, une consultation et une coordination étroites » en ce qui touche les activités de renseignement au Canada et à l'étranger. Fort de cette observation, le CSARS a recommandé que le SCRS adopte une interprétation plus large de son engagement à communiquer des renseignements au MAECI afin de permettre à celui-ci de se préparer à tout effet négatif qui pourrait découler d'opérations du Service à l'étranger.

Au cours de la Seconde Guerre mondiale, la Grande-Bretagne et les États-Unis ont travaillé en étroite collaboration à capter les communications de leurs ennemis, opération que l'on a appelée interception des signaux radio. En 1946, dans le contexte du début de la guerre froide avec l'Union soviétique, les deux grandes puissances ont décidé de consacrer cette coopération dans une entente officielle. Deux ans plus tard, le Canada a adhéré à cette alliance, suivi de la Nouvelle-Zélande et de l'Australie en 1956. Au fil des ans, les « Five Eyes » ont élargi leurs réseaux et leurs partenariats avec d'autres services, ce qui a amené à intensifier les échanges d'informations sur diverses menaces d'origine étatique ou non étatique contre les pays membres.

criminelles, ont contribué à faire des services canadiens de renseignement et de sécurité des partenaires clés du SCRS.

Au fil de cette étude, le CSARS a cerné une question que le SCRS devrait examiner au moment où il accroît sa capacité et ses activités de collecte à l'étranger. Le CSARS reconnaît l'importance d'une communication interministérielle efficace, notamment

cybermenaces. Cette sensibilisation s'impose et entre dans les fonctions d'enquête du SCRS, mais les efforts de sensibilisation ciblée risquent de devenir des activités qui pourraient être perçues comme une mesure d'atténuation. L'atténuation, qui vise les conseils prodigués aux victimes réelles ou éventuelles d'organismes gouvernementaux désignés, n'entre pas dans le mandat du SCRS quant à ce dossier. Le rôle du SCRS est sans cesse présenté comme un rôle d'appui, par ses activités d'enquête, aux efforts gouvernementaux d'atténuation que dirige le CSTC.

Le CSARS reconnaît que les activités de liaison sont complémentaires aux méthodes d'enquête du SCRS et lui fournissent des moyens de faire avancer son enquête sur les cybermenaces. Cependant, au moment où le SCRS s'emploie à suivre le rythme de ces menaces, il doit continuer de s'attacher à son rôle d'enquête et de se garder d'exercer des activités susceptibles d'être perçues comme des moyens d'atténuation.

ÉTUDE DU CSARS :

La relation du SCRS avec

un partenaire des « Five Eyes »

Pour remplir son mandat, il est essentiel à tout service de renseignement de coopérer avec ses homologues canadiens et étrangers. Cela est d'autant plus vrai depuis les événements du 11 septembre, les services de renseignement ayant dû resserrer leur coopération pour faire échec à une menace terroriste à l'échelle mondiale. Au Canada, le SCRS a reconnu que l'intensification de ses activités d'enquête à l'étranger a suscité un degré de coopération sans précédent avec ses partenaires étrangers.

Étude du CSARS

Les ententes du SCRS avec des services étrangers, qui sont à la base de ce travail de collaboration, lui permettent de coopérer et d'échanger des informations sur des enjeux d'intérêt commun. Le SCRS a conclu plus de 250 ententes avec des homologues du monde entier, les relations qu'il entretient avec ses partenaires, connus sous le nom de « Five Eyes », figurent parmi les principales d'entre elles.

La présente étude traite de l'histoire et de la transformation du rôle du Service au sein de la collectivité des Five Eyes dans un examen approfondi de la coopération et des échanges du SCRS avec un partenaire des Five Eyes. Le CSARS a complété cette étude par la visite d'un poste du SCRS à l'étranger, qui a chargé d'y gérer ces partenariats, et par des rencontres avec les homologues canadiens du SCRS à la mission du MAECI. Le Comité a constaté que, ces dernières années, l'évolution du contexte de la menace, les pressions budgétaires et les progrès technologiques ont souligné l'importance de la collaboration au sein de la collectivité des Five Eyes. Le CSARS a aussi constaté que la croissance des activités de collecte du SCRS à l'étranger a suscité un échange d'informations plus nourri sur les cibles d'intérêt commun au sein de l'alliance.

Dans son étude, le CSARS a constaté un degré élevé de coopération entre le SCRS et son partenaire des Five Eyes. De plus, la coopération et les préoccupations communes au sujet de questions courantes, telles la radicalisation, l'utilisation grandissante de l'Internet et les difficultés occasionnées par l'utilisation de plus en plus répandue d'informations dans les poursuites

Le CSARS a noté que le rôle du SCRS dans les enquêtes sur les cybermenaces est limité par son mandat, qui est de recueillir des renseignements sur les menaces contre la sécurité du Canada et de conseiller le gouvernement. Pour atteindre cet objectif, le SCRS a élaboré une approche à deux volets pour ses enquêtes sur le cyberspace :

premièrement, chercher à quel État imputer les cyberattaques contre le Canada et, deuxièmement, en comprendre les motifs.

Dans son étude, le CSARS a constaté que la migration des menaces d'espionnage dans le cyberspace a obligé le SCRS à redoubler d'efforts et, au fil du temps, à se doter de nouveaux pouvoirs et méthodes à employer dans le monde physique et virtuel. Par exemple, le SCRS a demandé une nouvelle gamme de pouvoirs que la cour octroie par la voie de mandats et qui vise à suivre le rythme du contexte entourant les cybermenaces, en évolution rapide, tout en fournissant des pistes d'enquête. Le CSARS a noté que la nouvelle approche du Service semble avoir établi des repères précis pour le succès futur des enquêtes sur le cyberspace. De surcroît, le SCRS s'est employé à optimiser les ressources opérationnelles déployées contre les cybermenaces.

Le SCRS est l'un des nombreux intervenants qui appuient les efforts de l'ensemble du gouvernement pour atténuer les cybermenaces. Le principal rôle en cette matière revient au Centre de la sécurité des télécommunications Canada (CSTC), qui a charge de protéger les systèmes et réseaux informatiques du gouvernement et de lui conseiller des moyens d'atténuer les risques. Le CSARS a constaté la collaboration très étroite du SCRS avec le CSTC, à résoudre les incidents touchant le cyberspace, et la complémentarité de leur travail.

À l'automne 2010, le gouvernement fédéral a présenté la « Stratégie nationale de cyber-sécurité » qui définit les rôles et responsabilités des ministères et organismes à l'égard d'un éventail de questions ayant trait au cyberspace, y compris l'espionnage virtuel. Compte tenu de son expertise et de son mandat, le Centre de la sécurité des télécommunications Canada (CSTC) joue un rôle clé. Selon la Stratégie, il est appelé à améliorer sa capacité de dépister les menaces et à faire face aux menaces et attaques virtuelles contre les réseaux de communication et les systèmes gouvernementaux de technologie de l'information. Pour sa part, le SCRS est appelé à enquêter et à conseiller le gouvernement sur les menaces contre la sécurité du Canada, dont les cybermenaces.

L'interception des signaux radio par le CSTC fournit des pistes d'enquête au SCRS, mais les renseignements que celui-ci recueille au fil de ses enquêtes peuvent améliorer la capacité du CSTC à faire face aux cybermenaces. Enfin, le CSARS a noté que le SCRS donne des séances d'information aux ministères fédéraux et aux organismes du secteur privé dans le cadre d'une approche « pangouvernementale » de sensibilisation aux

cyberespace pour forcer les réseaux de l'État et du secteur privé et faire main basse sur des secrets. Aussi est-il de plus en plus important de protéger le pays contre les cybermenaces, pour le gouvernement du Canada. Étude du CSARS La présente étude a trait à l'enquête du SCRS sur une cybermenace et, sur un plan plus global, à l'apport des efforts du Service pour la cybersécurité du Canada. Tout d'abord, le CSARS a examiné la nature de la cybermenace en question ainsi que certaines des principales difficultés associées à cette enquête. Il a ensuite étudié de plus près les stratégies et outils que le SCRS avait déployés pour faire progresser son enquête, notamment en ce qui concerne le recrutement de sources humaines. Enfin, le CSARS a exploré le rôle du SCRS dans une approche « pangouvernementale » plus vaste à la lutte contre les cybermenaces.

À la suite du 11 septembre, les services occidentaux de renseignement de sécurité ont concentré leurs efforts sur la lutte au terrorisme. Dernièrement, le directeur du SCRS a toutefois déclaré que l'espionnage a atteint au Canada un degré d'intensité comparable au plus fort de la guerre froide. En effet, des événements récents, telle la découverte d'un réseau d'espionnage russe aux États-Unis à l'été 2010, nous rappellent que la menace de l'espionnage demeure bien réelle.

L'évolution de la nature des activités d'espionnage, tout comme celles de terrorisme, complique le travail des services de renseignement. De nos jours, des personnes, des groupes et des services commandités par des États utilisent de plus en plus le

Mandats

Le pouvoir d'autoriser des techniques d'enquête intrusives appartient exclusivement à la Cour fédérale du Canada. En décernant un mandat au SCRS, la Cour l'autorise à recourir à des techniques d'enquête qui seraient illégales autrement, par exemple la surveillance de télécommunications. Le tableau qui suit montre le nombre de mandats que la Cour fédérale a octroyés au cours des trois derniers exercices financiers.

	2005-2006	2006-2007	2010-2011
Mandats nouveaux	26	36	55
Mandats remplacés ou renouvelés	183	193	176
Total	209 ¹	229	231

¹Ce chiffre comprend deux mandats urgents.

Troisièmement, le procès du « groupe des 18 de Toronto » a montré que les tribunaux canadiens sont prêts à contester les moyens, telle l'interception autorisée par mandat, que le SCRS emploie pour obtenir les informations qu'il communique à la GRC. Cela souligne l'importance de veiller à ce que le principe de la communication pleine et entière aux tribunaux, de tous les faits substantiels, soit consacré dans le processus des demandes de mandat du SCRS. Le SCRS estime que tous les employés du SCRS devraient bien comprendre l'obligation de divulguer tous ces faits de façon pleine et entière.

L'utilisation de renseignements de sécurité dans les procès criminels continuera d'évoluer à mesure que le SCRS et les organismes d'application de la loi apprendront à coopérer dans les enquêtes antiterroristes et que de nouvelles décisions judiciaires fourniront des orientations à cet égard. Le gouvernement fédéral pourra aussi donner d'autres directives. Dans sa réponse de décembre 2010 à la

« Commission d'enquête relative aux mesures d'investigation prises à la suite de l'attentat commis contre le vol 182 d'Air India », le gouvernement s'est engagé à prendre des initiatives visant à améliorer la relation entre l'utilisation des renseignements et leur application à titre de preuves dans les procès criminels. Le CSARS continuera d'examiner les relations du SCRS avec la GRC puisqu'elle en est le partenaire canadien le plus important.

Premièrement, le CSARS a étudié le système des deux types de notes (c.-à-d. de communication et d'instructions) que le Service emploie pour communiquer des informations aux organismes d'application de la loi. Une note de communication est généralement traitée comme un tuyau ou une piste d'enquête pour amorcer ou faire avancer une enquête criminelle, et la police ne peut s'en servir pour obtenir un mandat. D'autre part, la note d'instructions est le moyen officiel par lequel le SCRS autorise les responsables de l'application de la loi à utiliser ses informations dans leurs demandes de mandats à la cour.

Pour améliorer la qualité et la valeur des informations fournies par le SCRS à ses partenaires de l'application de la loi et rendre cohérente la manière dont il les leur communique, le CSARS a recommandé que le SCRS adopte un modèle de communication qui comporte une seule note intégrant les normes d'examen juridique rigoureux fixées actuellement pour les notes d'instructions.

Deuxièmement, l'importance de la coopération hâtive et fréquente, avec la GRC, est un point qui est revenu souvent. La coopération dans une enquête en cours suppose des échanges à de multiples niveaux, à la fois officiels et non officiels. Dans son étude, le CSARS a décelé des lacunes dans les dossiers du Service sur ses échanges opérationnels et stratégiques courants avec la GRC. Il est important que le SCRS consigne comme il se doit les échanges de vive voix, conformément à la jurisprudence récente sur la question de la conservation et à l'approche adoptée par le Service même en cette matière.

terrorisme peuvent constituer à la fois une menace contre la sécurité du Canada et un crime en vertu du *Code criminel*.

Au cours de la décennie qui a suivi, des informations ont été communiquées dans un nombre croissant de procès criminels, phénomène que certains ont qualifié de « judiciarisation du renseignement » ou de processus de « transformation d'informations en preuves ».

En 2008, le directeur du SCRS a déclaré publiquement que les services de renseignement avaient dû faire face à « diverses questions juridiques comme la divulgation, les normes de preuve et le témoignage du personnel des services de renseignements dans les poursuites au criminel », qui ont toutes eu des incidences profondes sur la mise en place et la conduite des activités de renseignement au Canada.

Étude du CSARS

Dans son étude, le CSARS a examiné la réaction du SCRS à l'utilisation accrue de renseignements de sécurité dans les procès criminels. Il a exploré la manière dont le Service et la GRC coopèrent, tout en respectant leurs rôles respectifs dans les enquêtes antiterroristes, et les leçons qu'on a tirées des récentes poursuites antiterroristes. Dans son étude, le CSARS a tout d'abord examiné le cadre qui régit la coopération entre la GRC et le SCRS ainsi que les

« Le CSARS a constaté l'instauration, par le SCRS et la GRC, d'un processus qui permet un partenariat efficace sur le plan opérationnel. »

approches et outils que celui-ci a élaborés, seul ou de concert avec la GRC, pour gérer cette importante relation. Le CSARS a constaté de grands progrès en ce domaine, notamment l'instauration, par le SCRS et la GRC, d'un processus qui permet un partenariat efficace sur le plan opérationnel. Le CSARS a ensuite examiné de plus près la manière dont cette approche avait été mise à l'épreuve au cours de l'enquête sur le « groupe des 18 de Toronto », l'une des premières grandes poursuites intentées en vertu de la *Loi antiterroriste* dans le système de justice pénale. De l'avis du CSARS, cette affaire a montré que le SCRS pouvait travailler efficacement avec la GRC sous le régime de cette nouvelle loi. Le CSARS a aussi examiné en détail deux jugements rendus par la Cour supérieure de la Justice de l'Ontario au cours des poursuites contre le « groupe des 18 de Toronto », s'attachant surtout à la coordination des opérations du SCRS avec la GRC et à ses échanges d'informations avec elle. Le CSARS a constaté que, dans l'ensemble, la réponse du Service à ces deux jugements aidera davantage à guider les futures enquêtes et poursuites antiterroristes. Compte tenu du fait que les discussions concernant le rapport entre renseignement et preuve ont toujours cours, le CSARS a souligné trois questions que le SCRS pourrait vouloir examiner de plus près.

l'expérience acquise, le CSARS a recommandé que le SCRS multiplie les efforts entrepris dans les bureaux régionaux en élaborant à l'échelle du Service une stratégie pour la gestion de ses relations avec le secteur privé. De l'avis du CSARS, pour que sa stratégie soit efficace, le Service devrait déterminer les secteurs les plus susceptibles de lui être utiles pour ses enquêtes.

Parallèlement, il y a des limites à ce que le SCRS travaille plus étroitement avec le secteur privé en raison des lois strictes qui régissent l'échange officiel d'informations. La *Loi sur le SCRS* ne l'autorise pas à communiquer les informations qu'il recueille à des partenaires non traditionnels ou non gouvernementaux, telles les entités du secteur privé. Selon l'article 12 de cette loi, la responsabilité du SCRS se limite à faire rapport au gouvernement du Canada des menaces contre la sécurité nationale et à le conseiller à cet égard. Il existe des politiques opérationnelles sur l'échange d'informations avec le secteur privé, mais elles sont restrictives, comme il se doit, et comportent des paramètres stricts quant aux types d'informations qui peuvent être fournies. Pour ces raisons, le Service s'efforce de s'engager à l'égard des besoins du secteur privé en matière de sécurité et de les appuyer autrement. Par exemple, il essaie de partager davantage d'informations non classifiées, notamment en participant au Centre intégré d'évaluation des menaces, qui produit des évaluations de la menace et les distribue au secteur privé, entre autres. Le SCRS a aussi entrepris d'accroître le nombre d'habilitations de sécurité individuel-elles dans le secteur privé afin de permettre

ÉTUDE DU CSARS :

Le processus de transformation en preuves des informations du SCRS

des échanges plus significatifs sur les questions qui ont trait aux menaces à la sécurité nationale. Enfin, le SCRS effectue les enquêtes qui concernent les demandes d'habilitation de sécurité provenant du secteur privé si un ministère ou un organisme fédéral, ou encore une autorité provinciale compétente, parraine ces demandes. En vertu du programme de filtrage lié aux sites sensibles, par exemple, le SCRS fournit des habilitations aux personnes qui ont accès à de tels sites, comme les centrales nucléaires et les aéroports internationaux, et à des événements spéciaux comme les Jeux olympiques d'hiver de 2010. Le CSARS continuera d'examiner les relations du SCRS avec le secteur privé dans ses études futures et, s'il y a lieu, il approfondira les questions soulevées dans la présente pour améliorer sa compréhension des avantages et des défis que comportent les relations du Service avec des partenaires non traditionnels.

Règles sur la communication d'informations concernant le renseignement de sécurité

La Loi sur la SCRS interdit la communication d'informations obtenues par le Service au fil de ses enquêtes, sauf dans l'exercice de ses fonctions en vertu de la Loi ou pour l'administration ou l'exécution de celle-ci ou d'autres lois.

L'article 19, en particulier, fait état des situations où cette communication est autorisée, soit si elle est :

- faite à des organismes d'application de la loi et à des fonctionnaires judiciaires dans le cadre d'une enquête ou d'une poursuite;
- faite aux ministres de la Défense nationale et des Affaires étrangères, ou à des fonctionnaires ministériels, et si les informations concernent la défense ou la conduite des affaires internationales du Canada;
- autorisée par le ministre de la Sécurité publique et considérée d'intérêt public.

Le CSARS a appris que le Service optait habituellement pour une approche plus coordonnée et stratégique afin de nouer des relations avec le secteur privé. Dans le but d'optimiser les ressources limitées dont on dispose pour ces activités et de tirer parti de

les services de police canadiens, les autres ministères et organismes du gouvernement du Canada ou les gouvernements ou institutions de pays étrangers. De nos jours, le SCRS se tourne aussi vers des partenaires non traditionnels, comme le secteur privé.

Étude du CSARS

Cette étude porte sur l'intensification des relations du SCRS avec le secteur privé dans le contexte de la sécurité nationale. Le CSARS a examiné les efforts généraux de liaison et de sensibilisation déployés par le Service, principalement au niveau régional, auprès d'entités du secteur privé. Le SCRS a deux programmes principaux qui donnent lieu à la majorité de ces interactions :

- le Programme de liaison et de sensibilisation publiques : séances visant à sensibiliser le secteur public au mandat du SCRS et à faire de celui-ci un point de contact pour les renseignements susceptibles d'être liés à la menace;
- le Programme de liaison et de sensibilisation : séances axées davantage sur des menaces particulières.

Le CSARS a conclu que les interactions du SCRS avec le secteur privé sont importantes et peuvent être utiles dans la poursuite de pistes d'enquête plus précises.

Le CSARS s'est penché sur quelques cas où le SCRS a pu miser sur ses relations avec le secteur privé. Dans l'ensemble, il a constaté qu'il est essentiel au SCRS d'établir des relations avec ce milieu s'il veut pouvoir tabler sur les informations du secteur privé. En particulier, le Comité a signalé les efforts en ce sens des agents de liaison du SCRS.

Dans cette étude, qui porte sur les stratégies, politiques et processus guidant l'utilisation de l'Internet par le CSARS, le CSARS s'est attaché principalement au rôle d'une unité spécialisée qui a vu le jour en 2001. Il a notamment examiné en quoi le travail de cette unité aide à trouver des pistes et à faire avancer les enquêtes. Dans son étude, il s'est aussi penché sur les informations recueillies en ligne par le Service.

L'étude du CSARS lui a permis de constater que l'utilisation de l'Internet par le CSARS est de plus en plus répandue. Il importe donc que le Service dispose des ressources nécessaires pour faire face à la charge de travail. À cet égard, le CSARS appuie les conclusions d'une vérification interne signalant l'importance de se pencher sur ces problèmes de ressources.

Le CSARS a constaté que, dans l'ensemble, l'approche du CSARS à l'égard de ses travaux en ligne est bonne et souple. Il a aussi noté que le Service avait élaboré des lignes directrices utiles pour certaines activités sur l'Internet. Ces lignes directrices regrouperont en un document de référence utile les leçons tirées et les pratiques exemplaires.

Le CSARS a cerné deux points concernant l'utilisation de l'Internet par le CSARS.

Le premier est que l'interaction du CSARS auprès des jeunes Canadiens s'intensifiera sans aucun doute tant que les extrémistes continueront d'utiliser l'Internet pour tenter de les radicaliser. En effet, une bonne partie des documents extrémistes affichés en ligne à des fins de recrutement et de radicalisation cible les jeunes, qui

constituent l'un des groupes d'utilisateurs d'Internet les plus nombreux au Canada et ailleurs dans le monde. Dans son étude, le CSARS ne prend toutefois pas le SCRS à partie d'avoir recueilli des informations en ligne. Il croit cependant que le Service doit porter une attention spéciale lorsqu'il traite des informations ayant trait aux jeunes. Le problème était le volume d'informations les concernant, que le SCRS conserve dans le cadre de ses rapports opérationnels. Le CSARS croit que le Service devrait bien faire comprendre à ses employés la nécessité de procéder avec une plus grande circonspection lorsqu'ils recueillent et conservent des informations au sujet des jeunes.

Le deuxième point est que le CSARS a souligné l'importance que le SCRS applique le critère de « la mesure strictement nécessaire » lorsqu'il recueille des informations en ligne et les conserve. L'Internet offre d'énormes quantités d'informations qui sont facilement accessibles, mais il faut veiller à ce qu'elles soient assujetties au même critère de « la mesure strictement nécessaire » que les informations recueillies auprès d'autres sources.

ÉTUDE DU CSARS : Les relations du SCRS avec le secteur privé

L'intensification de la collaboration avec des partenaires non traditionnels est une tendance croissante dans le domaine du renseignement de sécurité au Canada et dans d'autres pays du monde. C'est avec ses partenaires canadiens et étrangers du secteur public que le SCRS entretient des relations depuis toujours, par exemple avec

Utilisation de l'Internet par le SCRS

En l'espace d'une génération, l'information disponible sur l'Internet a connu un essor prodigieux. Aujourd'hui, il y a là un vaste média interactif qui offre un grand anony- mat aux gens qui communiquent en ligne. Le rôle croissant que les activités en ligne jouent dans la radicalisation des individus susceptibles de devenir des menaces pour les intérêts canadiens préoccupe toutefois de façon particulière les services de renseignement de sécurité et les organismes d'application de la loi. De nos jours, des personnes qui ne se sont peut-être jamais vues peuvent créer des réseaux, mobiliser des gens et planifier des activités constituant des menaces... et cela, sans

jamais sortir de chez elles. Pour celles qui représentent une menace contre le Canada et ses alliés, les activités en ligne jouent un rôle important à chaque stade de la radicali- sation, donnant accès directement à une idéologie extrémiste brute et permettant aux radicaux qui la partagent de sabotcher dans un anonymat presque complet.

En conséquence, les activités constituant des menaces sont passées à l'avant-plan de nombreuses enquêtes en matière de sécu- rité nationale. L'Internet en est venu à jouer un rôle opérationnel important dans les enquêtes du SCRS. Ainsi, les principales cibles au sein du « groupe des 18 de Toronto » ont été repérées au début par la surveillance des documents affichés sur le Web.

Ciblage

Si le Service a des motifs raisonnables de soupçonner un individu ou une organisation de représenter une menace pour le Canada, il doit d'abord ouvrir une enquête. Les chiffres qui suivent indiquent les nombres de cibles (arrondis à la dizaine la plus proche) sur lesquelles le SCRS a fait enquête au cours des trois derniers exercices financiers.



La reddition de comptes importe

Le CSARS est l'un des divers mécanismes qui visent à assurer la reddition de comptes au sujet du SCRS. Celui-ci doit aussi faire rapport de ses opérations par l'entremise du ministre de la Sécurité publique, des tribunaux, de l'inspecteur général du SCRS, des organismes centraux du gouvernement (p. ex. le Bureau du Conseil privé et le Secrétaire du Conseil du Trésor), du vérificateur général du Canada ainsi que des commissaires à l'information et à la protection de la vie privée du Canada.

Recommandations du CSARS

Chaque année, le CSARS demande au SCRS un rapport indiquant où celui-ci en est par rapport aux recommandations qu'il a formulées dans ses études et ses décisions relatives aux plaintes de l'exercice précédent. Ce rapport lui permet d'assurer un suivi de la mise en œuvre de ses recommandations et d'en vérifier les effets concrets sur le SCRS. Ce processus fournit aussi au Service l'occasion de répondre officiellement aux études et aux décisions du CSARS, contribuant par là aux discussions constantes entre le SCRS et le Comité.

Au cours de la précédente période d'étude (2009-2010), le CSARS a formulé douze recommandations portant sur un vaste éventail de questions. Le CSARS a le plaisir de mentionner que le SCRS a donné suite à plusieurs de ces recommandations. Par exemple, en réponse à celles formulées dans son étude sur les relations du SCRS avec des partenaires canadiens choisis de première ligne, celui-ci a repensé le principal outil qui lui sert à évaluer l'état de ses relations au Canada dans ses rapports, auxquels il envisage aussi d'ajouter une catégorie indiquant à quel moment les renseignements trouvés dans les rapports lui ont été fournis par ses partenaires de l'application de la loi. De plus, en réponse à la recommandation du CSARS voulant que le SCRS demande des directives au Ministère en ce qui touche le recours à la perturbation pour faire échec aux menaces à la sécurité nationale, le SCRS a répondu qu'il avait soumis la question à l'étude du ministère de la Sécurité publique.

<p>Lorsqu'il détermine les sujets à examiner, le CSARS prend en considération :</p> <ul style="list-style-type: none"> • les événements ou les faits nouveaux susceptibles de menacer la sécurité du Canada; • les priorités établies par le gouvernement du Canada en matière de renseignement; • les activités du SCRS qui pourraient avoir une incidence sur les droits et libertés individuels; • les questions cernées par le CSARS dans le cadre de sa fonction relative aux plaintes; • les nouvelles orientations et initiatives annoncées par le SCRS ou le touchant; • le rapport annuel classifié que le directeur du SCRS présente au ministre de la Sécurité publique. <p>Chaque étude fournit un instantané des actions du Service dans un cas particulier. Cette approche permet au CSARS de gérer le risque que comporte sa capacité d'examiner seulement un petit nombre des activités du SCRS une année donnée.</p> <p>Les chercheurs du CSARS consultent de nombreuses sources d'information lorsqu'ils se penchent sur des aspects particuliers des travaux du Service. Dans le cadre de ce processus, ils peuvent organiser des séances d'information avec des employés du SCRS et étudier les dossiers d'enquête sur des individus et des groupes, les dossiers de renseignements et les documents joints aux demandes de mandats. Le CSARS peut aussi examiner les dossiers ayant trait à la coopération et aux échanges opérationnels du SCRS avec des organismes et des partenaires étrangers et canadiens, entre</p>	<p>Au fil des ans, le CSARS a étudié un vaste éventail d'activités menées par le SCRS, tant au Canada qu'à l'étranger. Nous l'avons fait en examinant :</p> <ul style="list-style-type: none"> • les activités du SCRS dans ses divers postes autour du monde; • les activités et enquêtes des bureaux régionaux du SCRS; • la coopération et les échanges de renseignements de celui-ci avec ses partenaires canadiens et étrangers; • des méthodes opérationnelles particulières, tel le recours à des sources humaines et l'interception secrète de communications par le Service. <p>Les études du Comité contiennent des constatations et, s'il y a lieu, des recommandations. Elles sont remises au directeur et à l'inspecteur général du SCRS ainsi qu'à Sécurité publique Canada.</p>
--	--

Pour en savoir plus à propos des études antérieures du CSARS

Au fil des ans, le CSARS a examiné un vaste éventail d'activités du SCRS. La liste complète des études antérieures du Comité peut être consultée sur son site Web (www.sirc-csars.gc.ca).

A. ÉTUDES

Les études du CSARS visent à fournir au Parlement et à la population canadienne un tableau complet des activités d'ordre opérationnel du Service. Dans ses études, le CSARS examine la manière dont le SCRS exerce ses fonctions afin de déterminer si le Service a agi de manière irréprochable, efficace et conforme à la loi.

Les études du CSARS fournissent un examen rétrospectif et une évaluation d'enquêtes et activités particulières du SCRS. Notre programme de recherches est conçu de manière à englober un vaste éventail de sujets, et à le faire en temps utile et par thème.

Distinction entre contrôle et surveillance

À l'extérieur du Canada, les organismes de contrôle de services de renseignement, tels les comités spéciaux du Sénat et du Congrès des États-Unis, examinent en permanence les actions de ces services. Ils ont pour mandat d'évaluer les enquêtes en cours ou les décisions « en temps réel » et, aussi, ils suivent généralement de près le budget et l'administration. En conséquence, ces organismes peuvent avoir part au processus décisionnel des services de renseignement parce qu'ils ont le pouvoir d'infléchir les décisions au moment où elles sont prises.

Au Canada, par contre, le CSARS étudie les opérations passées du SCRS. Il ne prend part ni à ses décisions courantes d'ordre opérationnel ou administratif, ni à ses activités, et il n'est pas impliqué dans ces décisions. Les études nous donnent le net avantage de pouvoir évaluer pleinement le rendement du SCRS sans y avoir été mêlés d'aucune manière.

et des défis que représente la tâche consistant à concilier la nécessité de protéger les renseignements secrets avec celle de les communiquer aux corps policiers pour appuyer les poursuites criminelles.

Ces constatations ne sont que quelques-uns des points saillants de nos études. Les pages qui suivent contiennent les résumés détaillés de toutes les études effectuées au cours du dernier exercice.

Conclusion

Nous vous présentons ici notre conception du rôle que pourrait éventuellement jouer le CSARS, et les résultats de nos études à titre de contribution à un débat public sur la

sécurité nationale. En effet, le Parlement a conçu pour nous ce rôle consultatif en 1984 parce qu'il entrevoyait « l'importance vitale du rôle que le CSARS serait appelé à jouer dans le cadre du système de renseignement de sécurité », en veillant au besoin « à ce que certaines questions touchant la sécurité fassent l'objet d'un débat adéquat ». Si le gouvernement choisit de mettre en œuvre un système d'examen indépendant plus vaste à l'égard des organismes chargés de la sécurité nationale, le CSARS espère que ses opinions aideront les décideurs à apporter des améliorations à l'appareil de la sécurité nationale et à accroître la confiance que les Canadiens ont en celui-ci.

Sur un plan plus global, nous avons constaté que le rôle joué par le Service auprès des détenus afghans fournit des leçons qui pourraient s'appliquer à d'autres opérations à l'étranger. Celles menées outre-frontières le sont dans des circonstances uniques et présentent différents défis, mais le SCRS devrait veiller à ce que la gestion de ses opérations à l'étranger soit la plus conforme possible aux normes d'administration et de reddition de comptes observées au Canada. L'étude de cette année sur la coopération du SCRS avec un partenaire des « Five Eyes » a fourni un aperçu d'une autre dimension sur le travail du Service à l'étranger. Le CSARS a constaté que l'intensification des activités du SCRS à l'étranger requiert une approche mieux intégrée auprès de ses partenaires canadiens. En particulier, nous avons exhorté le SCRS à repenser la manière dont il informe régulièrement, de ses activités outre-frontières, le ministère des Affaires étrangères et du Commerce international (qui a la responsabilité ultime de gérer les relations internationales du Canada). L'échange d'informations et la coopération avec les partenaires canadiens sont manifestement des éléments centraux du travail du SCRS en matière de renseignement et reviennent donc tout au long des études de cette année. Le CSARS a examiné l'une des plus importantes relations du Service – avec la GRC – sous l'angle de l'un des plus grands défis contemporains de la collectivité du renseignement : l'utilisation de renseignements de sécurité à titre de preuves. Le Comité a conservé une bonne impression de la coopération entre la GRC et le SCRS et il s'est fort bien rendu compte de la complexité

pas les vastes réseaux qui ont depuis été établis pour faire échec à la menace terroriste à l'échelle mondiale. Jusqu'ici, le SCRS a réussi à fonctionner dans le cadre existant, mais le CSARS craint que ces lacunes ne commencent à grever l'efficacité opérationnelle du Service, sinon à l'amener à exercer des activités débordant son mandat. Parallèlement, le SCRS a modernisé ses techniques d'enquête traditionnelles afin de suivre le rythme des nouvelles menaces. Le CSARS a souligné ce processus dans son examen de l'enquête du Service sur les cybermenaces, qui sont passées au rang des principales priorités du gouvernement fédéral en matière de renseignement. Dans cette étude, le CSARS s'est penché sur les stratégies et outils novateurs que le SCRS a déployés pour faire progresser cette importante enquête. De même, dans notre étude sur l'utilisation de l'Internet par le Service, nous avons pu nous rendre compte de l'appui que ce moyen fournit à ses activités. Le CSARS a aussi donné suite à notre engagement à prêter davantage attention à la croissance des activités d'enquête du SCRS à l'étranger. Cette année, nous l'avons fait en examinant un dossier très public, soit le rôle du Service dans les entrevues de détenus afghans, et cela, dans le cadre de ses activités opérationnelles globales en Afghanistan. Le CSARS a conclu que le SCRS devrait évaluer avec soin et cohérence les informations émanant d'organismes susceptibles d'enfreindre les droits de la personne, et joindre des réserves à ces informations, préoccupations que le CSARS avait exprimées à l'occasion d'études antérieures.

publique et avec l'assentiment du ministre compétent. Ces légers changements seraient peu coûteux et pourraient aider à atténuer les préoccupations du public à l'égard du système existant au Canada en matière de reddition de comptes au sujet de la sécurité nationale.

L'étude de cette année sur le rôle du SCRS dans les entrevues de détenus afghans en est un exemple concret. Si le CSARS avait pu se pencher sur les actions des autres ministères intéressés, cela aurait donné un examen plus complet et, du même coup, aurait permis un rapport public plus vaste sur les activités menées par le Canada à l'étranger, en ce qui touche la sécurité nationale. Qu'il y ait ou non des changements structurels, le CSARS continuera de veiller à fournir, par ses études, l'évaluation la plus complète possible des activités du SCRS.

Devant l'évolution du contexte de la sécurité nationale, le CSARS a examiné les activités opérationnelles du SCRS sous des angles nouveaux et il a fouillé de nouveaux champs d'enquête. Il s'est aussi engagé à rendre publics son travail et ses constatations le plus possible, de manière à contribuer au débat public sur la sécurité nationale.

Observations du CSARS

« Devant l'évolution du contexte de la sécurité nationale, le CSARS a examiné les activités opérationnelles du SCRS sous des angles nouveaux et il a fouillé de nouveaux champs d'enquête. »

Dans cette optique, le rapport de cette année contient plusieurs études « de base » sur de nouveaux sujets, dont une sur l'évolution des interactions du SCRS avec le secteur privé. Le CSARS examine régulièrement les relations du SCRS avec ses homologues canadiens et étrangers et avec les autres partenaires du secteur public, mais pour la première fois nous avons choisi d'examiner en profondeur sa coopération avec le secteur privé. Dans son étude, le CSARS a conclu qu'en dépit de la tendance vers une coopération accrue avec le secteur privé, notamment avec les propriétaires et exploitants de certaines infrastructures essentielles du pays, la capacité du Service à travailler en étroite collaboration avec ce secteur commerciale d'importantes limites juridiques et pratiques.

Fait à noter, l'étude a révélé une lacune grandissante entre le cadre juridique du SCRS, instauré il y a trois décennies au plus fort de la guerre froide, et la réalité opérationnelle ultérieure aux attaques du 11 septembre. Lors de l'adoption de la *Loi sur le SCRS*, en 1984, on n'avait pas envisagé que le SCRS travaillerait en étroite collaboration avec des intervenants autres que des États. À cette époque, les activités de renseignement étaient en bonne partie axées sur la lutte aux menaces de l'espionnage et de la subversion et ne requéraient

sur des personnes. Par exemple, l'Agence des services frontaliers du Canada peut refuser d'admettre quelqu'un au Canada et CIC a le pouvoir de renvoyer un individu du Canada. Ces pouvoirs ne se comparent toutefois pas à celui du SCRS de recueillir des renseignements en secret, ce qui peut avoir une incidence directe sur les droits civils et libertés d'une personne, mais à son insu. Les puissants mécanismes de surveillance du SCRS visaient à faire contrepoids à sa capacité d'agir en secret, et cela, d'une manière qui pouvait affecter gravement la vie des intéressés. En conséquence, nous nous demandons si le même niveau d'examen permanent et indépendant s'impose pour les ministères et organismes dont les mandats ne prévoient pas de pouvoirs semblables.

Regard sur l'avenir – réorienter le CSARS

La *Loi sur le SCRS*, qui confère au CSARS le pouvoir et la capacité d'examiner à fond tous les aspects des activités et des opérations du SCRS, n'est pas « détraquée ». Pourtant, la nature et l'ampleur des changements au contexte du renseignement de sécurité nous amènent à nous pencher sur la structure canadienne de reddition de comptes quant à la sécurité nationale, et sur le rôle du CSARS à cet égard.

Le juge O'Connor a fait observer à juste titre que les activités de nombreuses entités fédérales, en matière de sécurité nationale, sont devenues assez intimement liées par suite des attaques du 11 septembre. C'est la une constatation que le CSARS souligne dans des études récentes. De nos jours, le SCRS assure une liaison constante et travaille en étroite collaboration avec

nombre de partenaires fédéraux, tendance qui ira vraisemblablement en s'accroissant du fait que ses activités s'intensifient et deviennent plus complexes au Canada et à l'étranger. Le CSARS examine à fond ces activités et fait rapport à ce sujet dans ses études et ses rapports d'enquête sur les plaintes. Le défi consiste à donner aux Canadiens le même degré d'assurance au sujet de l'ensemble des opérations du gouvernement quant à la sécurité nationale. Nous croyons que l'examen indépendant des activités du Canada concernant la sécurité nationale pourrait être amélioré en réorientant le CSARS, ce qui pourrait se faire sans aucune modification législative, dépense ou restructuration majeure. Cela donnerait un système proportionné, quoique efficace, d'examen indépendant général de la sécurité nationale.

Actuellement, dans le cadre de ses études, le CSARS ne peut examiner ni évaluer les questions de sécurité nationale qui ne relèvent pas du SCRS, même si les actions ou avis de celui-ci peuvent les influencer. Une légère modulation du mandat du CSARS pourrait combler cette lacune, permettant des études plus complètes sur l'échange d'informations et les interactions du SCRS avec ses partenaires canadiens. De plus, elle autoriserait le CSARS à examiner les actions des autres entités fédérales qui établissent des rapports avec le SCRS ou s'y associent. En outre, une modification mineure à la *Loi sur le SCRS* pourrait habiliter le CSARS à entreprendre une étude sur un ou plusieurs organismes autres que le SCRS, sous l'angle de la sécurité nationale, à la demande du ministre de la Sécurité

Cette année, le CSARS a intensifié ses activités d'intéressement du public afin d'atteindre un objectif qu'il s'était fixé dans son rapport annuel de 2009-2010, à savoir susciter le débat public sur le rôle futur du renseignement de sécurité et, à titre corollaire, sur la fonction de surveillance qui appuie ce rôle. Encore une fois, ces discussions ont porté sur ce thème : par suite des attaques du 11 septembre, le Canada a bénéficié d'une coopération opérationnelle bien meilleure entre les ministères fédéraux, au nombre de près d'une vingtaine, qui s'occupent de sécurité nationale.

Au Canada, pourtant, le système de freins et contrepoids, qui a été instauré il y a plus de deux décennies pour assurer la reddition de comptes de ces divers organismes, n'a pas suivi le rythme de ces changements. Les mécanismes de surveillance existants, dont le CSARS, ne sont ni conçus ni outillés pour examiner à fond les activités de plus en plus intégrées du Canada en matière de sécurité nationale. Parallèlement, de nombreux ministères et organismes actuellement chargés de la sécurité nationale ne sont assujettis à aucune forme d'examen indépendant.

Examen des activités du Canada en matière de sécurité nationale

Au cours des cinq dernières années, trois commissions d'enquête – O'Connor, Iacobucci et Major – ont fait état de questions concernant les activités du Canada en matière de sécurité nationale et toutes en sont venues à la même conclusion. La « Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar » (aussi appelée Commission O'Connor) a notamment entrepris un examen approfondi du cadre de responsabilité à l'égard de la sécurité nationale au Canada. Le juge O'Connor a proposé pour le CSARS un rôle très élargi en raison de son expertise de longue date dans la surveillance des activités ayant trait à la sécurité nationale. Le nouveau rôle du CSARS comporterait un examen indépendant et constant de ce type d'activités, et cela, pour quatre entités, outre le SCRS : le ministère des Affaires étrangères et du Commerce international (MAECI), le Centre d'analyse des opérations et déclarations financières, Citoyenneté et Immigration (CIC) et Transports Canada.

La principale question qui vient à l'esprit est la suivante : ces activités justifient-elles un examen permanent, indépendant et constant? Les activités des autres entités fédérales relativement à la sécurité nationale sont, bien sûr, susceptibles d'avoir une incidence

À propos du présent rapport

Le mandat et les fonctions du CSARS sont définis dans la loi même qui établit le cadre juridique du Service, à savoir la *Loi sur le Service canadien du renseignement de sécurité*. Conformément à cette loi, il prépare chaque année un rapport public sur ses activités, que le ministre de la Sécurité publique transmet au Parlement.

Le présent rapport annuel résume les principales analyses du CSARS ainsi que les constatations et recommandations qui découlent de ses études et de ses enquêtes sur les plaintes. Il compte trois sections :

Section 1	Bilan de l'exercice	Analyses des faits marquants, dans le domaine du renseignement de sécurité, et de leurs rapports à la fois avec certaines constatations et recommandations formulées par le CSARS lors du dernier exercice.
Section 2	Résumés des études du CSARS et des plaintes	Résumés des études effectuées par le CSARS et des rapports de plainte qu'il a présentés durant l'exercice financier visé par le présent rapport.
Section 3	Survol du CSARS	Exposé des activités du CSARS en matière d'intéressement du public et de liaison et sur le plan administratif. Les détails de son budget annuel et de ses dépenses y sont présentés.

publique, et nous y sensibilise, tandis que notre condition d'indépendance nous permet d'agir en toute impartialité. Les Canadiens s'attendent à ce que notre travail transcende les événements et la politique, et nous continuerons de veiller à ce qu'il en soit ainsi.

Le rapport de cette année vise encore une fois à engager les parlementaires, et en fait tous les Canadiens, à l'égard de diverses questions importantes, pertinentes au renseignement de sécurité. Notre « Bilan de l'exercice » et nos « Résumés des études du CSARS et des plaintes » (les sections 1 et 2, respectivement, du présent rapport annuel) mettent ces éléments en lumière. Nous espérons avancer la réalisation de l'objectif

énoncé dans le rapport de l'an dernier, à savoir susciter le débat public entourant le rôle futur et les défis du renseignement de sécurité ainsi que la fonction de surveillance à l'appui de ce rôle. Dans le contexte de la menace aujourd'hui aggravée, il importe que le service de renseignement de sécurité du Canada ait le pouvoir et la capacité d'enquêter sur les nouvelles menaces. Et, fait tout aussi important, ces activités doivent être menées dans un cadre qui permet une reddition de comptes appropriée. La sécurité collective ne doit pas être assurée aux dépens des droits et libertés individuels et le CSARS maintiendra ce principe clair à l'avant-plan de son travail.

Les membres du CSARS (de gauche à droite) :

l'honorable Denis Losier, l'honorable Frances Lankin, l'honorable Dr Arthur T. Porter (président), l'honorable Dr Philippe Couillard et l'honorable Carol Skelton.



Message des membres du Comité

SCRS. Le présent rapport annuel résume les fruits de nos travaux, dans la mesure permise par la loi.

Le mandat du Service est demeuré inchangé depuis sa création, mais son travail est parvenu à un niveau de complexité que l'on n'avait pas entrevu il y a 25 ans, ce qui est inévitable dans un monde où les menaces se multiplient à un rythme parfois effarant sur la scène internationale.

Tout en modulant la manière dont il déploie ses ressources pour faire face à ces circonstances nouvelles, le CSARS ne s'est pas dérobé aux tâches fondamentales que le Parlement lui a confiées en 1984. Notre travail, tel que nous l'entrevoyons, consiste à évaluer les faits observés de façon indépendante, méticuleuse et équitable, et à fournir au gouvernement des conseils et des recommandations à propos, en nous fondant sur ces évaluations.

Dans la mouvance de l'opinion publique et le rythme rapide des événements et des changements à l'échelle mondiale, le rôle et la nature du CSARS prennent une importance spéciale. En notre qualité de membres, nous apportons une expertise considérable et diverse à notre travail, ayant servi dans diverses branches du secteur public, soit la politique, la médecine, l'administration publique et les organisations non gouvernementales, pour ne nommer que celles-là. Cette expertise nous fait prendre conscience collectivement des questions d'importance

Susciter et maintenir la confiance dans les institutions publiques sont les principes sur lesquels repose une société libre et démocratique. C'est là une tâche particulièrement difficile s'il s'agit d'une institution qui ne peut faire l'objet d'un examen public rigoureux parce qu'une bonne partie de son travail doit être menée sous le couvert du secret. Tel est le cas du Service canadien du renseignement de sécurité (SCRS) qui a charge de recueillir les renseignements ayant trait aux menaces contre la sécurité du Canada.

Depuis plus de 25 ans, le Comité de surveillance des activités de renseignement de sécurité (CSARS) s'emploie à veiller à ce que cette puissante entité réponde de ses actes devant le Parlement et les citoyens du Canada. La même loi qui a instauré les pouvoirs juridiques relatifs aux activités du SCRS a aussi créé un système détaillé de freins et de contrepois à l'égard de ses pouvoirs. Le rôle du CSARS est donc de contribuer à assurer que le Service respecte les droits fondamentaux et les libertés des Canadiens lorsque celui-ci enquête sur les menaces à la sécurité nationale.

En particulier, le CSARS veille à ce que le SCRS exerce ses fonctions dans la légalité et d'une façon efficace et appropriée. Il s'y emploie par un examen continu des activités du SCRS et par l'enquête des plaintes contre le Service, ainsi qu'en formulant des conclusions et des recommandations au ministre de la Sécurité publique et au directeur du

Table des matières

MESSAGE DES MEMBRES DU COMITÉ 2

À PROPOS DU PRÉSENT RAPPORT 4

SECTION 1 : BILAN DE L'EXERCICE 5

SECTION 2 : RÉSUMÉS DES ÉTUDES DU CSARS ET DES PLAINTES 10

A. ÉTUDES 10

Utilisation de l'Internet par le SCRS 13

Les relations du SCRS avec le secteur privé 14

Le processus de transformation en preuves des informations du SCRS 16

L'enquête du SCRS sur les cybermenaces 19

La relation du SCRS avec un partenaire des « Five Eyes » 21

Le rôle du SCRS dans les entrevues de détenus afghans 23

La méthode d'évaluation de la fiabilité des sources humaines par le SCRS 25

B. PLAINTES 27

Présumé comportement inadéquat de la part du SCRS 29

Retard présumé à fournir une évaluation de sécurité 30

Évaluation présumée injuste, sans fondement et contraire à l'éthique, d'un demandeur de résidence permanente 31

SECTION 3 : SURVOL DU CSARS 32

Composition du Comité 32

Personnel et organisation 32

Activités du Comité 32

Liste des recommandations du CSARS 34

À propos du CSARS

Le Comité de surveillance des activités de renseignement de sécurité (CSARS ou Comité) est un organisme indépendant qui rend compte des opérations du Service canadien du renseignement de sécurité (SCRS ou Service) au Parlement du Canada. Le CSARS effectue des études sur les activités du SCRS et enquête sur les plaintes du public contre le Service. Cela lui permet de fournir au Parlement et à tous les citoyens du Canada l'assurance que le SCRS enquête sur les menaces contre la sécurité nationale et fait rapport à ce sujet d'une façon qui respecte la primauté du droit et les droits des Canadiens. Pour plus de renseignements sur le CSARS, veuillez consulter www.sirc-csars.gc.ca.

À propos du SCRS

Le Service canadien du renseignement de sécurité (SCRS) a charge d'enquêter sur les menaces contre le Canada, d'analyser l'information et de produire des renseignements. Pour protéger le Canada et ses citoyens, le SCRS conseille le gouvernement fédéral au sujet des questions et activités qui menacent ou pourraient menacer la sécurité nationale. Il effectue également des évaluations de sécurité pour le compte de tous les ministères et organismes fédéraux, sauf la Gendarmerie royale du Canada.

Un cadre juridique pour le CSARS et le SCRS

Depuis la *Loi sur le SCRS*, le Canada est devenu l'un des premiers pays démocratiques du monde à doter son service de sécurité d'un cadre juridique. Cette loi a défini clairement le mandat et les limites du pouvoir de l'État en matière de renseignement de sécurité et elle a instauré des mécanismes de responsabilité permettant de contrôler ce pouvoir considérable. Voilà un modèle qui a su résister à l'épreuve du temps, dans l'ensemble.



Le 30 septembre 2011

L'honorable Vic Toews
Ministre de la Sécurité publique
Chambre des communes
Ottawa (Ontario)
K1A 0A6
Monsieur le Ministre,

C'est pour nous un plaisir de vous remettre le rapport annuel du Comité de surveil-
lance des activités de renseignement de sécurité pour l'exercice 2010-2011, tel qu'il
est prescrit à l'article 53 de la *Loi sur le Service canadien du renseignement de*
sécurité, afin qu'il soit transmis au Parlement.

Veuillez agréer, Monsieur le Ministre, l'expression de notre haute considération.

Arthur T. Porter, C.P., M.D.

Président

Philippe Couillard, C.P., M.D.

Frances Lankin, C.P.

Carol Skelton, C.P.

Denis Losier, C.P.

Comité de surveillance des activités
de renseignement de sécurité
B.P. 2430, succursale D
Ottawa (Ontario) K1P 5W5
613-990-8441

Veuillez consulter notre site Web à www.sirc-csars.gc.ca

© Travaux publics et Services gouvernementaux Canada 2011
Numéro de catalogue PS 105-2011
ISSN 1921-0566



Freins et contrepoids

Le renseignement de sécurité sous
l'angle de la reddition de comptes

